2014

Using Radio Frequency Identification Technology In Healthcare

Sr. Avery Williamson

North Carolina Agricultural and Technical State University

Using Radio Frequency Identification Technology in Healthcare

Avery Williamson Sr.

North Carolina A&T State University

A thesis submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Department: School of Technology

Major: Information Technology

Major Professor: Dr. Li-Shiang Tsay

Greensboro, North Carolina

2014

The Graduate School
North Carolina Agricultural and Technical State University
This is to certify that the Master's Thesis of

Avery Williamson Sr.

has met the thesis requirements of
North Carolina Agricultural and Technical State University

Greensboro, North Carolina
2014

Approved by:

Dr. Li-Shiang Tsay Major Professor	Dr. Dewayne Brown Committee Member
Dr. Ibraheem Kateeb Committee Member	Dr. Clay Gloster Department Chair

Dr. Sanjiv Sarin
Dean, The Graduate School

Biographical Sketch

Avery Williamson Sr. earned his Bachelor of Science degree in Industrial Technology (Electronics) from North Carolina Agricultural and Technical State University in 1987. He is currently pursuing his Master of Science degree in Information Technology from North Carolina Agricultural and Technical State University.

Mr. Williamson has co-authored 2 papers. One paper was co-authored with Dr. Li-Shiang Tsay and Dr. Seunghyun Im entitled "Framework to Build an Intelligent RFID System for Use in the Healthcare Industry" that was submitted in the Technologies and Applications of Artificial Intelligence conference of 2012. It has been submitted in the IEEE archives. The second paper "Solutions for RFID Smart Tagged Card Security Vulnerabilities" was co-authored with Dr. Ibraheem Kateeb, Dr. Li-Shiang Tsay, and Dr. Dewayne Brown and was submitted in the 2013 AASRI Conference on Intelligent Systems and Control. The paper is included in AASRI Procedia (ISSN: 2212-6716).

While pursuing his degree Mr. Williamson worked as a Network Engineer for Sprint Nextel and Ericsson and is currently a Wireless Switch Network Planner for Sprint. He is responsible for performing long-term capacity planning for the Samsung 4G EPC equipment in the Sprint LTE network.

Dedication

I dedicate this thesis to my wonderful family. To my wife LaShawn, who has encouraged me through this journey and to my five children; Avery Jr. Joel, Amber, Noah, and Lyndon who have motivated me to be an example by showing them that they must never stop learning. Finally, I dedicate this work to my late father Clemon Williamson and my late mentor Bishop Otis Lockett Sr. These two men encouraged me to pursue living a life that embraced my full potential and destiny. I am thankful to God for placing them in my life.

Acknowledgements

It could not have been possible to write this thesis without the help and support of my wife LaShawn Williamson. I am deeply appreciative of her support and affirmation as I embarked on this journey through graduate school.

I would like to thank my advisor Dr. Li-Shiang Tsay who helped me through this process. There were many days when I wanted to quit but her persistent discipline and encouragement was a great inspiration for me especially when I had to juggle work and school. Her dedication to higher education and hard work has been a great example for me. I would also like to thank Dr. Dewayne Brown and Dr. Ibraheem Kateeb who graciously agreed to be on my advisory committee along with Dr. Tsay. I am deeply appreciative for all that you have done.

Table of Contents

List of Figures

List of Tables

Abstract

In the healthcare industry, medical treatment can be a matter of life and death, so that any mistakes may cause irreversible consequences. As hospitals have sought to reduce these types of errors, Radio Frequency Identification Technology (RFID) has become a solution in the healthcare industry to address these problems. Since 2005, RFID has generated a lot of interest in healthcare to make simpler the identification process for tracking and managing medical resources to improve their use and to reduce the need for future costs for purchasing duplicate equipment.

There are rising concerns linked to the privacy and security issues, when RFID tags are used for tracking items carried by people. A tag by its design will respond to a reader's query without the owner's consent and without the owner even noticing it. When RFID tags contain patients' personal data and medical history, they have to be protected to avoid any leaking of privacy-sensitive information. To address these concerns, we propose an Intelligent RFID System which is a RFID card system that embeds smart tags in insurance cards, medical charts, and medical bracelets to store medical information. Patient data is sent to the insurance providers by way of a clearinghouse that translates the information from the healthcare facility into a format that the insurance company can process. To ensure data protection, an additional security layer was added to secure the communication between the tags and the readers. This security layer will allow only authorized readers to poll tags for the patient's medical tags and prevent unauthorized access to tag data. It will simplify the maintenance and transfer of patient data in a secure, feasible and cost effective way.

CHAPTER 1

Introduction

Healthcare treatment can be a matter of life and death, so that any mistakes may cause irreversible consequences. With an aging population combined with better and more extensive health care, people are provided improved medical service. As a result, healthcare systems are dealing with the demanding task of making their level of performance to deliver enhanced care in a more efficient way. Information and Communication Technology (ICT) and its use in healthcare have been researched at length to address this challenge. Different ICT solutions have been developed to assist medical organizations in sharing critical information about patients, to enable patients to monitor their health, and to prevent errors in medications. ICTs have been proven to be beneficial tools that are able to advance the quality of healthcare service and reduce, or at least, control costs [1].

One of the benefits of ICT is the implementation of Automatic Identification and Data Capture (AIDC) techniques. These techniques could not only offer fast and easy identifying, tracking and tracing objects or people but also can collect data automatically. Once the data is retrieved, it can be stored directly to a computer system, eliminating human errors. This is essential to the performance of operational tasks and business intelligence analysis. Such technologies are mainly used in healthcare for identification to improve patient point of care and reduce miscalculations. These methods include barcodes, Radio Frequency Identification (RFID), etc.

When barcodes were implemented it helped automate and standardize the identification process. A barcode is usually used to identify product information; but, it does not offer sufficient data to fully describe the product. Its use involves an operator to place a barcode reader

next to the barcode to read information. In addition, the bar code cannot be reused since its information cannot be changed.

RFID utilizes wireless communication technology to provide the ability to uniquely recognize objects or people using devices called tags. The RFID system is made up of three critical parts: a tag, a reader and a host system. The RFID tag and reader talk on a specified radio frequency. When an object that has a RFID tag goes in the communication area of the reader, the reader tells the tag to send the data that is stored on it. After the reader accumulates the data from the tag, it sends the data to the RFID controller by a network connection (Ethernet, Mobile IP, etc.). The controller will take the information and use it depending upon on the type of data it has received. The data can be stored in a database or moved as an object in inventory.

Unlike the barcode, RFID tags can keep information regarding the individual product. Also, the RFID readers can scan information on many products at the same time repeatedly, without needing direct line of sight for reading the tags. Additional advantages of the RFID technology are the reading range, easy data transmission between a receiver and a transmitter, reusability and data security [2]. Because RFID has a better automation level of tracking and tracing processes that are supported by higher data integrity and accuracy, they offer real-time reaction capabilities and end-to-end visibility compared to the barcode technology. RFID technology is expected to substitute barcodes in the near future [3]. Since 2005, there has been much attention in using RFID to sustain healthcare services among the variety of existing ICTs. Healthcare is generally considered as RFID's next major adopter [4].

Most RFID applications in healthcare are centered on identification, tracking, and tracing of patient, medicines, operating equipment, and medical personnel. The main purpose of these applications is to automate manual processes and to bring down the amount of time, cost of

tracking, locating assets, (including supplies and people) in hospitals. Eventually, it enhances patient safety and permits healthcare professionals to be more efficient in their work. Although RFID has great potential to handle medical data effectively and efficiently, the general acceptance of RFID in healthcare beyond pilot implementation and testing has faced many barriers, particularly concerning data security and patient privacy. To address these concerns, a new tool that can simplify the maintenance and transfer of patient data in a secure, feasible, accurate and cost effective way is significantly needed.

1.1 Objective

The objective of this thesis is to prevent medical misidentification by proposing an Intelligent RFID System which is a RFID card framework that embeds smart tags in insurance cards, medical charts, and medical bracelets to store medical information. In this study the following goals are to be addressed by such system:

- The patient is correctly identified.
- The patient's medical data is protected from outside threats.
- The patient is safe from the medical errors caused by patient misidentification.

This system cannot prevent human error that may cause a misdiagnosis but provides enough checks and balances that can possibly catch and prevent them from occurring.

Embedding RFID smart tags in insurance cards offers several advantages for patients, healthcare facilities and insurance companies. For the patient, their medical data such as blood type, allergies to medicine, and prior medical history is stored on the smart tag along with their health insurance coverage information. With this data available, the patient does not have to verbally give their medical information whether conscious or incapacitated and is protected against misidentification. The advantage for the health care provider is that they can treat the

patient faster because the patient's medical information is readily accessible. This solution also allows the provider to keep the patient's medical information updated as they receive treatment. For the insurance companies, they are notified immediately when the patient enters the facility and are updated as the patient receives treatment through the clearinghouse. The companies accept the correct billing information from the health care providers for patient treatment and are notified when the patient is discharged. The assumption of this study is that every person will carry an insurance card.

1.2 Approach

In this thesis, the research has been based on existing RFID solutions that have been implemented commercially and what is being currently utilized in the health care industry. The present benefits and limitations were examined in the investigation of existing RFID systems and the information was used to propose the smart tagged insurance card system. RFID security threats and countermeasures were also reviewed. This data was utilized in proposing the security solution for the tag and reader communication link for the system.

1.3 Organization

The thesis is organized as follows: Chapter 2 gives a historical background on the development of RFID technology, the components of the RFID system, and an overview on how a RFID system works. It also reviews the developments in RFID technology that were its major cause of growth and the main attributes of the technology. It examines the current use of RFID in the commercial industry and looks at future RFID applications. The benefits of using RFID technology in healthcare are discussed along with the problems faced with implementing it in the health care industry. Chapter 3 provides an overview of the medical errors that healthcare facilities currently experience and looks at the problems with the process flow between hospital

department such as the Emergency Room, Inpatient, and Outpatient treatment. It also shows how RFID is currently being used in medical applications in health care facilities. In this chapter the framework for the RFID smart tag (or Intelligent ID) insurance card system is presented. The structure is defined along with the system components and how such system would work. Reader capacity models for hospitals are recommended to support the framework. Existing RFID solutions are reviewed and compared to the proposed system. Chapter 4 examines RFID security, the threats that face RFID technology, countermeasures that are available, and propose a security solution for the RFID Intelligent ID system. Recommendations are also made for reader capacity for hospitals for the security framework. Chapter 5 completes the thesis with the questions that are still open and provides a guide for future research and discussion.

CHAPTER 2

Literature Review

2.1 RFID Technology Review

RFID stands for Radio Frequency Identification and utilizes wireless communication technology to provide the ability to distinctively identify objects or people using devices called tags. RFID technology has been around for years and people have been using it without really knowing what it is. The technology is based on scientific theories of electromagnetic radiation from the 19th century. RFID is built upon radio signals and radar technology and the first well-known use of it was in World War II in the identification, friend, or foe (IFF) system [5] [15]. This system was created by Great Britain to identify if detected aircraft were friendly or an enemy. It used radar to send a signal from a base to an arriving plane that would activate its radio transponder. If the plane was theirs, the transponders would send a secret code that showed that it was a British aircraft. If the plane sent the incorrect code or did not respond at all, it was perceived as a possible threat.

Today the use of RFID is common because of its everyday applications. This technology is made of three fundamental parts.

1. The RFID Tag – This is also identified as a transponder. It is made of a semi-conductor chip, an antenna, and a battery (depending upon on the type of tag).
2. The RFID Reader – The RFID reader is also called an interrogator or a read/write device. It consists of an antenna, an RF electrical element, and a control electronics element.
3. The RFID Controller – This component can consist of a computer workstation that has a database and management (or middleware) software.

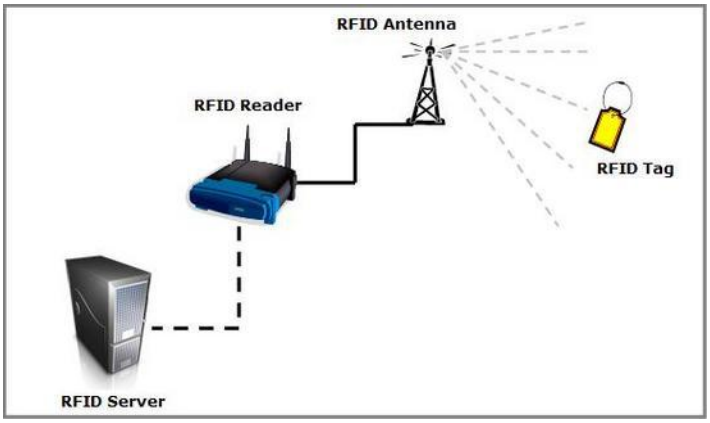

Figure 1. RFID system

(Source: http://www.instablogs.com/indian-schools-all-set-to-implement-rfid-and-gps-based-tracking-system.html [74])

The RFID tag and reader talk to each other on a specified radio frequency. When an object that has a RFID tag goes into the communication zone of a reader, the reader tells the tag to send the data that is stored on it. After the reader collects the data from the tag, it sends the data to the RFID controller by a network connection (Ethernet, Mobile IP, etc.). The controller will take the information and use it depending upon on the type of data it has received. It can store it in a database or move the object into inventory.

A system using RFID can be made up of many readers in a localized area and be connected to one controller. A reader can also have the ability to communicate to multiple tags, with the tags having the ability to be connected to nearly anything (from merchandise on a shelf, a medical ID bracelet, or a pallet).

2.1.1 RFID Tag Types. The work of a RFID tag is to contain and send data to the reader. Its components are a computer chip, memory and an antenna at its most basic level. The electronic chip has memory that stores data that is read from and can be written to depending

upon on the function of the tag. The tag may also have a battery which is related to the type of tag (Active or Passive) [5] [15].

The computer chip receives and processes data from the RFID readers and uses the memory to give the special identifier for the tag. Each tag has a special identifier that makes it unique from other tags.

The antenna in the tag allows communication to the reader and helps to broaden the communication range between tag and reader. The way the antenna is designed is based on the tag's application and the location it is used. A good system design will help the tag and reader communicate properly. A poor design will cause misreads and terrible reliability.

RFID tags can be categorized into different classes. Each class denotes the capability of the tag. Table 2 describes the functions for tag classes [15].

Table 1

Tag Classification

(Modified from Source: RFID Applied [15])

Tag Class	**Function**
Class 0/1	Have a passive operation. Class 0 tags are factory-programmed. Tags that have functions past Class 1 are user-programmable.
Class 2	Have encryption and are read-writable.
Class 3	Have internal batteries, greater range and can communicate on a wider range of frequencies.
Class 4	Have an active operation, can perform peer to peer communications and provides more sensing abilities.
Class 5	Have enough power to trigger other tags and can also be categorized as a reader.

When a RFID tag has a battery or an internal power source, it is determined to be an active tag. When data needs to be transmitted to the reader, the tag uses the power source to obtain the

power needed to send the data to the reader. Active tags can send data over long ranges over hundreds of feet and can communicate with readers with less power. They normally have a larger memory size which can go up to 128K. These tags are bigger and more intricate than passive tags which cause them to be more costly to build.

A passive RFID tag does not have an internal power source. It uses power from the radio signaling from the RFID reader. Passive tags are cheap to manufacture and can be very small in size. Passive tags have a smaller range than active tags with ranges less than 2 feet. They also need readers with stronger signaling and have small memory size up to a few KB.

The semi-active tag is a tag that has the characteristics of the active and passive tag. This type of tag has batteries but do not use them in data transmission. It receives energy from the radio signaling from the reader and then uses the battery to transmit data from the tag. The battery can also be used to give power to a different function on the electronics chip. When the battery function is not needed, it goes into the sleep mode to conserve power and prevents unnecessary transmitting from the tag when it is not needed.

Another type of tag that is in an experimental phase is called the harmonic or Microwire tag and has been created by Demodulation Inc [15] [51]. This tag is the size of a human hair and is a formless alloy encased in glass like the fiber in a fiber optic cable. The alloy carries the information and when it is hit by the carrier wave from the RFID reader, it transmits the data. It is very cheap with the cost ranging around $0.01. The researchers believe that it can be incorporated with established tags to increase the read communication distance and also make the tag size smaller.

2.1.2 RFID Memory Types. RFID tags also can vary with the types of memory they can contain. Tags can have two kinds of memory: read-only (RO) and read/write (RW).

Tags with RO memory can only be used as read only and programmed one time. Once they are programmed they cannot be changed. This type of tag contains data that is fixed (equipment serial or part numbers) and can be incorporated into existing systems.

Tags that are read-write (RW) are called smart tags and have the ability to contain more data and memory that can be expunged and re-written multiple times. This allows the tag to have its own database, which allows it to contain information and become independent of the RFID controller or host centralized database. Smart tags can merge sensing capabilities, dynamic information, and communication because of the ability to contain more data and memory than read-only tags.

RFID tags can be created in several different forms because the components that make up the tag can be manufactured on a very small scale. The form of the tag can now be based on the type of application for which it is manufactured.

2.1.3 RFID Readers. RFID readers are miniature computers that have three basic components; an antenna, an RF electronic element that talks to the RFID tag, and a manager electronic element that handles communications with the RFID controller or host workstation. The main functions of the RFID reader are; to read the data of the RFID tag, write data if it is a smart tag, send data to and from the RFID controller, and send power to a tag that is passive. Advanced readers can also utilize anti-collision actions to guarantee parallel read-write communication for multiple tags at the same time, provide authentication to eliminate fraudulent activities and prohibit unwarranted access to the host systems, and provide the encryption of data.

Because RFID does not need a line of sight for the tags and readers, the RFID system has flexibility as far as the location of the readers. They can be placed in fixed locations, such as

doorways, ceilings, and shelves. The portable readers can be installed in any type of items that are moving, including hand-held units that can go to locations outside of the main facility. For the sake of this research, we could use an ambulance or fire trunk as a location for a portable unit.

Due to advancements in computing technology RFID readers are becoming smaller and cheaper in cost. Reader manufacturer are producing readers that can fit on a computer chip. In the future, a reader will be located on its own chip, thus allowing for lower prices and also more processing power for the readers.

Readers are also being developed to operate in multifrequency ranges. This allows the equipment the capability to receive radio signals in two or more frequencies. A multifrequency reader would be able to pull data from tagged items that have different frequencies. For example in the healthcare field, a reader could pull personal data from smart tagged insurance cards that are from different health insurance companies. This type of reader will have the ability to read a wider range of tags from different manufacturers.

2.1.4 RFID Controllers/Middleware. For the RFID system, the RFID controllers are the main management element. The hosts provide connectivity for many RFID readers; contain the main database, and system software. It is usually a PC or computer workstation and can utilize the information from the readers in various forms depending on the type of data being retrieved.

RFID middleware is the software that runs on the host system that manages the RFID readers. This software provides the ability to access and modify reader settings and can permit operators to upgrade the reader software remotely. Middleware provides the capability to allow monitoring on the functionality of the readers in the network and is an essential part of the data

collection process. Middleware can perform the database function and assists in the performing tracking, reporting, and storage of the data being retrieved from readers.

2.1.5 Operating Frequencies. RFID systems can communicate in multiple frequency bands. Banks et al (2007) in their book "RFID Applied" provide a table that shows the frequency ranges for Low, High, Ultrahigh, and Microwave frequency banks and their common uses in RFID technology [15]. Table 3 provides the listings of RFID frequencies and uses for each frequency range.

Table 2

RFID Frequencies

(Modified from Source: RFID Applied [15])

Frequency Range	**Common Frequency**	**Common Uses**
LF—Low frequency	30 kHz 125 kHz 134.2 kHz 300 kHz	Access control Animal identification Lot identification Chemical process use Distribution
HF—High frequency	3 MHz 13.56 MHz (ISO 15693) 30 MHz	Logistic warehouse mgmt Auto manufacturing/tracking Retail Hospitals Baggage check Library management Parcel tracking Security Smart cards
UHF—Ultrahigh frequency	300 MHz 433 MHz 866 MHz (Europe) 915 MHz (United States)	Retail Toll roads Logistics—Inside a factory and through the supply chain Long-range applications Item tracking
Microwave frequency	2.45 Gigahertz 3.0 Gigahertz	Long-range applications Item tracking Freight tracking

Lower frequency RFID has a lesser cost and better penetration; however, it suffers from a shorter transmission distance, slow data transmitting rate and a larger superficial area of antenna than higher frequency RFID [11]. In the healthcare industry, the frequency bands for RFID usage are 13.56 Hz for passive tags and 900 MHz UHF for active/passive tags [6].

2.2 RFID Applications

Radio Frequency Identification (RFID) technology is a communications system that uses wireless technology to identify objects. The use of RFID technology is increasing because it is becoming cost effective to implement due to technological advances. Since the inception of RFID 50 years ago, over 1 billion RFID tags have been sold throughout the world. It is estimated that by 2015 approximately 1 trillion tags could be sold.

The growth of RFID technology is largely due to Wal-Mart and the U.S. Department of Defense. According to Hunt et al (2007) in "RFID-A Guide to Radio Frequency Identification", Wal-Mart started requiring their main merchandisers to tag their pallets and cases with RFID tags to allow inventory tracking at the pallet level. After this, the Department of Defense asked its main suppliers to follow suit. Because of the size of both organizations, their requests for suppliers to use RFID created an expansion and brought it into the commercial mainstream [5] [15].

The subsequent developments in RFID were major causes of growth for the new technology and were crucial in the framework of expansion of RFID in the industry. Brown (2007) notes the following developments for growth:

- Standardization of protocols.
- Price of RFID tags decreased.

- Higher-frequency technology was being made available.
- Ability to send and receive data at faster data rates was being developed.
- Ability for RFID readers to read multiple tags in the same read zone simultaneously was being demonstrated.
- Software was being made available that would use data generated by RFID.
- Growth of the internet as a major part of companies IT infrastructure, allowing tags anywhere to communicate with readers in close proximity.

The major attributes of RFID technology is its capacity to identify, locate, track, and monitor people and objects without a line of sight between the tag and reader. The way that these capabilities are addressed characterizes how the RFID application is developed in industries where data is accumulated. There are three factors that have to be considered as RFID technology is implemented commercially. These factors have to be evaluated to determine the effectiveness of the RFID application in the commercial setting [5] [15];

- Power – Does the tag have its own power source or is it activated by the reader's electromagnetic field? Is this enough for the commercial requirements?
- Read Range – What is the read range of the tag? Does the tag need to be close to be read?
- Capacity for Storage – Does the tag have the storage needed for use in the commercial requirement?

Commercial business areas will be the main focus of growth for RFID technology. Hunt et al (2007) gives a listing of business sectors where RFID is currently being used and how much the technology's use has grown in our society today [5]. Table 4 provides the breakout of the sectors and the associated use of RFID technology.

Table 3

Commercial RFID Applications

(Modified from Source: RFID-A Guide to Radio Frequency Identification [5])

Business Sector	**RFID Commercial Application**
Transportation and Distribution	Fixed Asset Tracking: Aircraft, Vehicles, Rail Cars, Containers Equipment, Real-Time Locations Systems
Retail and Consumer Packaging	Supply Chain Management: Carton Tracking, Crate/Pallet Tracking, Item Tracking, Pharmaceuticals, Inventory and Tracking
Industrial and Manufacturing	Manufacturing: Tooling, Work-in-Progress
Security and Access Control	Tracking (animal and children), Facility Access, Airport and Bus Baggage, Anti-Counterfeiting, Computer Access, Employee Identification, Forgery Prevention, Branded Replication, Parking Lot Access

The commercial use of RFID technology that will cause continued growth is inventory tracking at the pallet and crate level. RFID manufacturers will focus on development in areas that will increase the amount of use for RFID technology. As RFID use increases, the cost to implement the technology will be reduced and spur a greater demand for it. The potential market expansion for RFID is dependent upon the cost to implement and maintain the technology. There are several problems that hinder RFID growth; the high costs associated with implementing a RFID system, the need for global standards, and security/privacy issues associated with the technology. RFID use in the commercial business sector is proving to be effective. The technology is being used for toll-road payments, airport bag tracking, shipyard port container tracking, paying for merchandise, and for passport use.

Many states that have toll-roads use RFID technology for driver payment. During the mid-90's, RFID toll systems had been developed to function at speeds where drivers can drive without interruption through tolls without any interference. Also the technology grew to the point

where drivers could pay many tolls using the same bank or credit card account. The E-Z Pass Interagency Group in the northeast United States is an agency that uses this technology.

The McCarran International Airport in Las Vegas uses RFID technology for baggage processing. Because the Transportation Security Administration required baggage screening, the airport management found that the use of RFID smart-labels were an effective way to track and screen bags going in and out of the airport. The airline employees put RFID tags on luggage when they are checked in and the system sends the bags to the explosive detector and then to the airplane for loading. Since implementing this system the airport show the increase of a 99.5 accuracy rate in baggage handling.

The Port of Singapore employs RFID technology to track shipping cargo containers. It uses RFID tags embedded in the ground to produce a grid system that allows for a three-dimensional way to track the cargo units. Tags are also placed on the containers and readers are positioned on forklifts and trucks. Because they are being monitored in three dimensions, the port management can easily locate any container when needed with a zero loss rate.

American Express has created ExpressPay which uses RFID to provide a contactless way to make daily purchases. A RFID tag is embedded in an American Express card or an attachment to a key chain and the transaction is made as a credit or debit card payment. This system is used for payment transactions that are quick and convenient with no signature needed by the card holder. It can be used in supermarkets, gas stations, restaurants, or places where purchases can be transacted in a speedily fashion.

In 2006, the United States State Department started embedding RFID chips in passports. The information on the chips held the passport holder’s name, address, picture, and biometric

information. The purpose was to make passports secure, harder to forge, and limit the passports use if it was lost or stolen.

2.3 Future RFID Applications

As the use of RFID grows, the impact will be seen in every aspect of our society. Automotive tires in the United States are being tagged to meet the terms of the United States Recall, Enhancement, Accountability, and Documentation Act in order to monitor tire usage [18]. The airline sector is implementing RFID technology for inventory tracking on aircraft parts to better improve safety. In the home, RFID is being used to monitor household appliances, such as refrigerators, and washer/dryers, to let consumers know when to buy more groceries or what type of detergent to use. Human tag implants are being tested to monitor body functions, as well as, to lock and unlock car doors.

In the next chapter, RFID use in the healthcare will be reviewed. An analysis of current issues that hospitals face will be reviewed along with the barrier facing the implementation of the technology. We will also present the Intelligent RFID solution that can potentially address those issues.

.

CHAPTER 3

RFID Intelligent ID System

3.1 Common Medical Mistakes in Hospitals

Approximately 98,000 patients die every year from medical mistakes that can be preventable [9]. Common medical mistakes are patient misidentification, inaccurate diagnosis, wrongly prescribed medication, and surgical errors.

Patient misidentification is one of the leading causes of medical errors and is the most common problem that healthcare facilities especially hospitals face. This type of medical error is a grave threat to patient safety. Research has shown that a large number of medical errors that are created by undesirable drug incidents are caused either directly or indirectly by patient misidentification [7] [10].The problem here is that identifying patients can be taken too lightly by hospital staff. This is simply because of the large number of interactions they have with patients. Because of this, healthcare providers may be not be aware that misidentification has taken place. Table 1 shows the types of problems that can be caused by patient misidentification [10].

Table 4

Consequences of Patient Misidentification

(Source: Modified from Positive Patient Identification using RFID and Wireless Networks [10]*)*

Receiving the wrong medication
Having the wrong medical procedure performed
Treatment delay on the right patient due to the mislabeling of medicine, hospital wristbands, samples of blood/tissue, or food tray
Incorrect diagnosis given to patient
Wrong patient sent to surgery
Cancellation of treatment due to improper filing of medical records

Inaccurate diagnosis is another form of medical mistakes that occur in the healthcare industry. Approximately 40,000 to 80,000 patients die due to being wrongly diagnosed by healthcare providers [7]. There are several causes for inaccurate diagnosis and are noted below [12]:

- Medical tests that are not ordered, followed up, accurately read, or postponed by the patient.
- Medical referrals not occurring due to lack of patient follow through or the specialty doctor fails to report findings back to main doctor.
- Patients not continuing their follow up appointments.
- Medical equipment failure
- Initial inaccurate diagnosis by doctor.

In order for doctors to come to an accurate diagnosis, they must have access to the required clinical knowledge. Physicians need a system in place to receive input from their fellow doctors to be given advice on their clinical abilities.

Another medical error that is detrimental to patients is wrongly prescribed medication. This type of mistake takes the lives of more than 100,000 people every year [7] [13]. Medication errors are in the top 10 leading causes of death in the United States. The major cause of wrongly prescribed medication is human error. Doctors can prescribe the right drug but because of their handwriting the pharmacist makes the wrong prescription. The pharmacy can receive the correct information from the doctor's office but writes the information down wrong. The doctor can also mix up patients and prescribe the wrong medication to one that should go to the other.

The last medical error under discussion is surgical errors. Medical mistakes involving surgical errors cost the medical industry approximately $1.3 billion dollars in medical payout over a 20 year period [7] [12]. This type of error includes medical sponges left in patients, having the wrong procedure performed, and the wrong patient is getting surgery. The most common error is surgical sponges being left behind in patients.

3.2 Common Hospital Process Problems

There are three main areas that make up a healthcare system in a hospital. Those areas are accident and emergency, inpatient ward, and outpatient care [15]. Patients entering into accident and emergency are evaluated and taken care of based on the seriousness of their situation. Their treatment is normally handled quickly and are either released or referred to inpatient care. Residents that enter into inpatient care have a more extended time of treatment. Those that are admitted into outpatient care are passed on for appointments with specialty doctors and can have same-day treatment. Because of this process flow, the patient information, records, and resources tied to the management of patient's treatment are passed around internally within each specific area and between the three areas. Banks et al (2007) in their book RFID Applied shows in Figure 2 the process flow for each area.

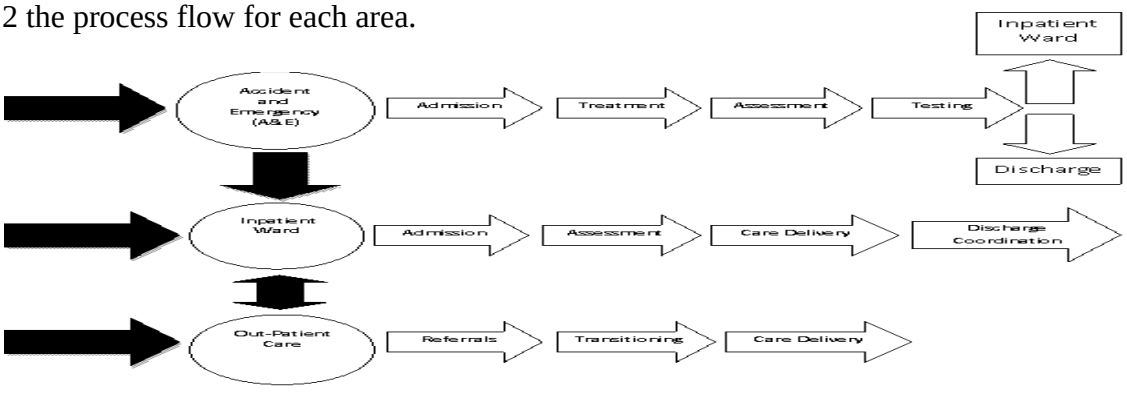

Figure 2. Process flow for patient treatment

(Modified from Source: RFID Applied [15])

A hospital's accident and emergency room provides treatment to those with severe wounds or in need of emergency treatment. It functions in a 24 hour/365 day operation. Patients can either be given medical treatment speedily or may have it delayed due to the severity of the injury. Some of the problems facing this department are;

- Time to review patient cases
- Ensuring that patients have proper treatment
- Transporting the patients to next phase of treatment in inpatient care.
- Inadequate communication between departments that cause delays with patients that need inpatient care have rooms or when a patient needs to be discharged.

The hospital inpatient departments receive their patient intake from the emergency room and are treated by a team of doctors and nurses. The patient's medical information is kept by notes or computers. Some of the issues seen in inpatient care are ensuring that there are enough beds for patient admittance, the time it takes to develop accurate patient medical records, and the delay in releasing patients for discharge due to the lack of planning.

The hospital outpatient care department handles patient discharge for outpatient care. This covers making sure those patients have their needed medication after treatment or being sent to medical specialists for further treatment. Some of the problems seen in this department are receiving inadequate patient medical records from the hospital inpatient or emergency departments and making sure that the appropriate medical resources are available for the referred patients.

3.3 Benefits of Using RFID in Healthcare

In the healthcare industry, we have found several benefits that RFID creates. These benefits help to save patient lives by eliminating medical mistakes, savings to time and cost, and an increase in efficiency.

The main objective for utilizing RFID technology in the healthcare industry is to enhance patient safety. RFID has great potential for providing patient information and location rapidly to increase the accuracy of identifying the patient and the medication being prescribed for treatment. Patient information can be contained in wearable RFID tags and the patient is monitored so that the location and any medicine prescribed to the patient are known. RFID can also allow for monitoring of alerts due to healthcare provider error. For example, if surgical equipment is left in a patient after surgery, the surgical staff could be alerted that the equipment is there and further harm could be averted.

Another benefit that RFID technology provides is the savings to time and costs. RFID is used to track and monitor medical assets, thus preventing the theft and loss of equipment. Also since the medical equipment is tracked, doctors and nurses have easier access to the equipment and can treat patients efficiently. The result is increased staff productivity and quicker treatment for patients. This can cause a savings of $1 million dollars a year for a small hospital [11] [17].

RFID also creates an increase in efficiency by providing the ability to automate the way medical data is retrieved. Procedures that use manual processes can now be automated with the way data can be stored and captured. It also produces operational improvements in the way that patients are cared for from admission to being released from medical care.

3.4 Barriers to Implementing RFID in HealthCare

There are several barriers that hinder the RFID adoption in the healthcare industry. These barriers severely impede the use of RFID in commercial business as well as the healthcare industry. Several factors have to be taken into account in order to deploy RFID technology in healthcare. These factors are technological, economical, and privacy/security.

3.4.1 RFID Technical Limitations. The technical limitations noted impact the use of RFID overall and particularly impacts its use in healthcare. Some include physical limitations that impact the accuracy of a RFID reader when it tries to discover a tag that comes into its read area. These limitations are noted below [5] [15].

- Reader Interference – When the signals from different RFID readers overlap, it causes collisions between readers and interference.
- Environment – Several environmental conditions impact RFID reader accuracy. Some items such as metal can have an effect on high and low frequencies that the readers and tags are transmitting on. RFID equipment can affect other medical equipment by interference especially if they transmit on the same frequency.
- Tag Location – The placement of RFID tags on an item can affect reader accuracy depending on its rotation angle.
- Distance and Power – The differences in distances between tags and readers can cause setbacks for those that design RFID systems. RFID signal transmissions that travel through different materials can create large changes in power and diminish accuracy.

Another technical constraint is the ability for a RFID reader to discover multiple tags at the same time. This is called RFID scalability. RFID scalability is dependent upon the computing muscle of the reader and the computer network it is attached to. There has to be adequate

computing resources to provide the ability to manage collisions between the RFID tags. At this time of this study, there is an issue with the anti-collision methods used in RFID technology. This is causing the readers a problem with not being able to handle multiple tag collisions. The lack of scalability currently impacts the spread of RFID in the healthcare arena as well as other industries. The anti-collision issue can be addressed if the readers and computer network have sufficient computing power to support the number of tags that are deployed for the system.

Managing the data that produced by the RFID tags is another technical limitation is another factor that may be faced by those organizations implementing the technology. Although there will be a huge quantity of data that will be created by RFID, back-end databases and applications must be able to handle this massive load. Many IT departments are overlooking the impact that RFID will have on their network infrastructure. There are several challenges that healthcare organizations will face regarding the data produced from RFID. These systems will create large quantities of data in short periods of time. The IT infrastructure must be designed to accommodate it. Healthcare organizations that have centralized IT locations will have to deal with the issue of administrating the raw data and at the same time transmitting it to the centralized locations. The IT networks must be able to handle extremely large volumes of data that will be transmitted through them. If not, these networks will not be able to manage the data flow and inevitably impact other mission critical applications that could endanger patient safety and facility operations.

Another technical barrier is the lack of a global standards and guidelines for RFID technology. There is a considerable difference internationally in regards to the frequencies and power levels for RFID systems. This is due to every national government possessing the right to decide which RFID spectrum ranges to use. When there is such a difference internationally, the

RFID system in one country may not work in another. RFID primarily operates in the UHF band which is where the most advances in the technology are being seen; however, the spectrum allocation in this band is also where the most disparities are seen. If there is not an international agreement on RFID spectrum and other guidelines, there is less of a chance that there will be interoperability between the different RFID systems, which will lead to the lack of growth of RFID technology. One of the reasons behind the lack of global adoption is that there are disagreements between standards and regulatory organizations. Companies that produce RFID equipment receive royalties on their own RFID systems and do not want to lose the royalties if they go to standardized systems. These problems can be addressed in two ways. First international standards must be created for the technology. Secondly companies that receive royalties on their own RFID systems can adopt licensing fees per tag if they move to standardized systems. This option will allow them to continue to profit from their equipment.

3.4.2 RFID Economical Limitations. The first economical barrier to RFID adoption is the cost of purchasing and implementing a RFID system. One of the issues with implementing RFID technology is the cost of RFID tags. In 2007, the cost of RFID tags was between $0.30 and $0.60 [5]. In 2010, the cost of a passive tag was $0.10 and an active tag was several dollars [17]. The increase in the use of RFID technology is dependent upon how much the price for RFID tags will drop in the years to come. Another issue is the cost to build a RFID system. There is a significant cost in purchasing the tag readers and supporting backend systems as well as designing a total RFID solution. Because RFID is a relatively new technology, those that could manufacture RFID components and those that would adopt the technology may be reluctant to fully implement it because of the possibility of risk associated with any new technology and they may be unwilling to invest in RFID. This is a normal risk for companies that upgrade or

implement new IT systems. They must be able to weigh the long-term savings over the cost of installing RFID technologies.

3.4.3 RFID Privacy/Security Limitations. Healthcare providers that use RFID technology will only see its advantages if the patients are convinced that the data being transferred is secure and will not be abused. Because the RFID tag holds unique identifiers that are connected to personal information, the healthcare industry must make sure that the RFID data transmission is highly secure. RFID security will be discussed in Chapter 4 of this research.

There are several essential characteristics of RFID that are significant to privacy, that is not limited to the technology, type of application, or the way the RFID system is deployed [25].

- RFID systems are a very important part of the healthcare provider's information system and there must be an overall approach for privacy for the entire system and not just focus on the air interface between card and reader.
- The unique identifier contained in the RFID tag can be correlated to the patient's personal information and involves privacy issues because of this.
- RFID tag information can be retrieved without the patient having knowledge of it. This creates issues for patient consent.
- RFID systems can retrieve time and location information which allows correlation to the patient's personal information. This can be used as surveillance data depending on who is pulling the information for their use.

These characteristics show how much personal information is handled by a RFID system and the important of protecting this information.

3.5 RFID Implementation in HealthCare

In order to address the issues mentioned in the preceding paragraphs, RFID technology is being used in a variety of healthcare applications to make the industry more successful. There are a number of advantages to using it in the healthcare industry and they are noted below [18].

- Tags do not need a line of sight to transmit data.
- Development of reusable active tags.
- Real-time availability to medical information.
- Ability to identify assets, equipment, patients, and staff without visual and physical contact.
- Ability to have security control with tracking and tracing means.
- Ability for better resource management.

Several areas where RFID technology is implemented in the healthcare industry are asset tracking, identification and verification, and monitoring. This section will provide a brief overview of how RFID is being used in those areas.

Asset tracking is an area where RFID technology is utilized the most in the healthcare industry. Medical equipment is being tracked to prevent theft and to locate needed equipment for medical use. RFID is being implemented to track drugs to reduce drug counterfeiting, prevent theft, and stop medication abuse. It is also being used to track patients that cannot take care of themselves such as; dementia patients, blind and hearing impaired, and children. RFID technology can also be used to locate medical providers at emergency locations in a disaster and those who are injured. Several countries are using RFID technology in a variety of ways for asset tracking to be more efficient in providing healthcare. In the United States, Southern Ohio Medical Center has implemented the Radianse Reveal Asset Tracking platform for asset and

equipment tracking. Also Bon Secours Richmond Health System has been using one of the largest RFID mobile asset management programs in the U.S. healthcare sector since 2004. This system handles asset tracking and management for critical medical equipment for three hospitals [24].

Identification and verification is the next area where RFID is being used in the healthcare industry. As stated earlier, medical errors kill approximately 98,000 patients each year. One of the main causes for medical mistakes is wrongful identification of the patient. Some ways that are being used to identify patients is the use of smart patient ID such as wristbands that contain patient information including name, date of birth, admission information, and surgical location [17]. In Italy's National Cancer Institute and Ospedale Maggiore hospital in Bologna, RFID technology is used to manage the blood transfusion process. RFID tags are installed on the blood bags and wristbands for patients. Medical staff have RFID ID cards and PDAs to record patient information when they arrive, confirm the blood type of the patient, and identify patient and blood group units when needed [24].

Monitoring is another area which RFID technology is being used. It is being used to monitor the patient's vital signs and the environmental conditions where patients are being kept. RFID is being tested to create alerts and triggers when a patient's vital signs reach a dangerous level and to also alert medical personnel when a patient's medical dispenser reaches a low state and need to be replenished. To reduce the hazard of having medical equipment being left in patients, RFID tags are being embedded in medical equipment so that after a medical procedure is completed, the patient can be scanned to check if any equipment is left in the patients. In Jacobi Medical Center in New York, medical personnel use tablet PCs to correspond the RFID tags on the patient wristband with bar-coded data on the patient medication. This system makes

certain that the patients are given the correct dosage of medicine and has only received what was prescribed to him or her. It also generates an electronic record of the personnel's visit [24].

3.6 RFID Intelligent ID System Proposal

Because RFID has great potential to handle medical data and can create a great benefit for patient safety and medical efficiency, we are proposing a RFID intelligent ID system utilizing smart tags embedded into insurance cards, medical charts, and patient wristbands to store information. This data is transmitted to the patient's insurance company when they enter the facility and is updated upon discharge. We are also recommending a clearinghouse that takes the patient information from the healthcare facility and translates it into a format that the insurance company can process. It will create a simpler way to maintain and transfer customer data in a way that is secure and cost effective [26].

3.6.1 RFID Smart Tags for the Intelligent ID System. For this system, we are recommending RFID smart tags to be used because of the storage capabilities and their ability to be overwritten multiple times. This permits the data on the card to be updated on a continual basis as changes occur. RFID smart tags are now being used in ATM Visa cards, passports, and toll collection devices.

The availability of battery powered tags is one reason why RFID smart tags were chosen to be utilized in our framework. There are several trends that have developed that have increased the feasibility of using battery powered tags [58].

- The development of low-cost CMOS RF Integrated Circuits (RFIC) and microcontrollers allow for cheaper tags.

- The price of batteries is getting lower. Inexpensive thin-film batteries are becoming accessible. These types of batteries are integrated in tags that are embedded in cards or active labels.

Another reason why battery powered tags were selected was because of the increased battery life. The battery technology developed now for smart tags can cause the tags to last 10 years [52]. The smart tagged cards will only transmit data when polled by the reader which assists with increasing battery life. Energy is conserved when the tag in the card is not transmitting. Because of these factors, the smart tagged insurance cards need only to be replaced when there is a malfunction, cards are lost or stolen, or when the battery life is depleted.

Battery powered tags also have a longer communication range. This will help especially if a person being admitted to the hospital is incapacitated or as patients are moved throughout the medical facility. The embedded smart tags in the medical charts assigned to the patients can be polled or updated as they move into different areas such as when the patient leaves the emergency room to their assigned rooms. Because of these factors, the insurance cards and medical charts in the Intelligent ID system with embedded tags provide great benefits to ensure correct patient identification. It also works to make sure that the correct medication and treatment is received by the patient.

3.6.2 Intelligent ID System Framework. The system framework consists of smart tags embedded into personal health insurance cards. The information on the cards will not be available unless it is placed inside a unique card reader under government oversight. It will be issued to healthcare providers that are registered for its use. The health insurance card was chosen for its size and its availability since patients with insurance carry it with them when they go to a healthcare facility. One of the advantages is that cards do not need to be replaced when

the patient changes insurance companies. They only need to be updated with the new insurance company information. The medical data on the card can assist the healthcare provider by maintaining the patient's medical information and transmit it when needed in a transferable format.

Figure 4 shows the framework for the system. The smart tag on the insurance card contains the medical data of the patient. The medical data would include the following information such as; date of birth, age, height, weight, and any medical conditions. The medical information would contain data such as; any allergies, type of medication being prescribed, current aliments, and the insurance coverage for the patient. Once the patient comes into a healthcare facility for treatment, a RFID reader retrieves the medical data from the smart tag in the insurance card and transmits the data to the facility database. Then it is then transferred to the health insurance company's database through a clearinghouse or third party that translates the healthcare facility data into a format that the insurance company can process and keep in data storage. As the patient is being prepared for treatment, their medical data is uploaded to a chart that has a smart tag embedded in it. The patient is also fitted with a wristband embedded with a smart tag. The wristband tracks the patient's medical treatment and health condition. When the treatment is finished, the medical chart and wristband sends the updated information to application servers that sends the data to the healthcare facility database and also the data is sent to the insurance company's database. This is done for billing through the clearinghouse so that the insurance company can process the updated medical data. The medical chart and wristband embedded smart tags are erased for reuse and the smart tagged insurance card is updated with the new medical data of the patient for possible future treatment.

This system can provide several advantages for the healthcare industry. It will help avoid the problem of patient misidentification by having two ways to identify the patient before and during treatment. The embedded smart tags in the medical chart and wristband are used to verify the patient's correct identity and can stop him or her from receiving incorrect medication or treatment. If there is a disparity between the chart and the wristband, an alarm is created for further investigation to find how it occurred and decide on the proper treatment. This system also provides cost reduction for the healthcare provider. When RFID is combined with a robust IT infrastructure, it produces a capable workflow for billing and reduction in paperwork.

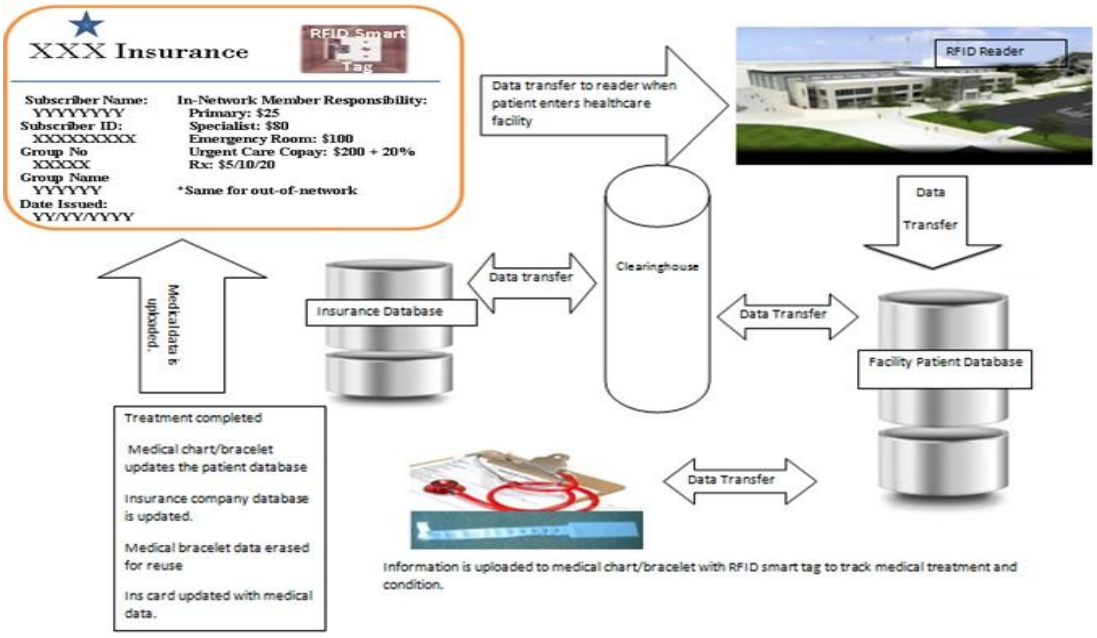

Figure 3. Intelligent ID System Data Process Flow

Since the medical data from the insurance card is transferred to the RFID reader automatically, the patient admittance and discharge procedure becomes the verification process. Also, the healthcare providers can give quicker treatment to the patient because the patient's medical data is easily accessible.

3.6.3 Intelligent ID System Operational Description In this section we will review how the system would work and possible design scenarios. There are several medical facility models to consider for our system. Table 5 gives a summary of brief survey performed on the local hospitals in Greensboro, North Carolina. For our survey 2 questions were asked.

- What is the bed capacity of your facility?
- What is the estimated number of patients seen in your emergency room daily?

Table 6 summarizes the bedding capacity and the estimated number of patients in emergency rooms for the hospitals located in metropolitan areas. Based on the data in both tables, it is noted that the average number of daily ER patient traffic for the local and metro hospitals is basically the same. Because of the similarities, this data is used for our hospital sizing models for our framework. The patient traffic (number of patients seen, admitted, and discharged) will determine the amount of readers that will need to be deployed in the facility.

Table 5

Local Hospital Sizing Survey Results

Name of Facility	Number of Beds	Estimated Number of Patients seen in ER Yearly	Estimated Number of Patients seen in ER Daily
Moses Cone Hospital	527	89,245	245
Wesley Long Hospital	171	56,210	154
High Point Regional	351	63,081	173
High Point Medical	N/A	27,010	74

Table 6

US Metropolitan Hospital Capacity

(Modified from Sources: http://health.usnews.com/best-hospitals/area [78] and http://www.cnn.com/2013/07/16/health/best-hospitals-ranking/index.html [79])

Name of Facility	City	Number of Beds	Estimated Number of Patients seen in ER Yearly	Estimated Number of Patients seen in ER Daily
Mount Sinai Medical Center	New York, NY	1,031	98,044	269
Massachusetts General Hospital	Boston, MA	945	89,475	245
Thomas Jefferson University Hospital	Philadelphia, PA	930	112,962	309
John Hopkins Hospital	Baltimore, MD	912	84,946	233
University of Maryland Medical Center	Baltimore, MD	819	68,518	188
Houston Methodist Hospital	Houston, TX	884	46,651	128
UCLA Medical Center	Los Angeles, CA	466	44,466	122

Table 7 shows the capacities of several RFID readers in the marketplace today. This data includes the reader type, manufacturer, reading range, the number of tags identified per second, and method of communication to the host systems. We will use this information to attempt to pair the reader capacity with the hospital sizing models in order to determine the type and capacity of readers that will be needed for patients entering hospital emergency rooms. The data will also be used in an effort to ascertain the type and capacity of readers needed to support the smart tagged medical charts and RFID wristband for patients admitted to the medical facility.

Table 7

RFID Reader Capacity

(Modified from Sources: http://www.alibaba.com, http://www.rfidinfotek.com, and http://www.atlasrfidstore.com [75] [76] [77])

Type of Reader	Manufacturer	Read Range	# of Tags ID per Sec	Communication Interface
Long Distance Reader DL5510	Unknown	10-40cm	30~50	Unknown (Assume 10/100 Ethernet
Omni-directional Active RFID Reader	Aerospace Innotech	~100cm	200	10/100 Ethernet, 802.11
Integrated Reader	ThingMagic	9m	400	10/100 Ethernet, 802.11
M6 UHF RFID Reader (4 Port)	ThingMagic	9m	750	10/100 Ethernet
Enterprise RFID Reader	Alien	No data available	2500	10/100 Ethernet, 802.11

When the patient enters a medical facility such as an emergency room, they will enter into the zone of the RFID reader. The type of RFID reader needed at the point of entry will be determined by the number of patients served by the location. For example, if all of the local hospital locations serviced at least 200 or more emergency room patients daily it would equate to approximately 8 patients an hour. The Long Distance Reader DL5510 that can scan 30 to 50 tags per second would be more than enough to handle the traffic. If the larger metropolitan hospitals, handled at least 500 patients daily in their respective ERs, it would equate to around 21 patients an hour. Again the Long Distance Reader DL5510 readers could be sufficient to handle their emergency room patient traffic. Table 8 shows the possible pairing of reader capacity to hospital ER patient traffic. The assumption is that for smaller hospitals would potentially see at 50 to 100

people daily and for larger facilities the number could be 100 or more. These numbers will fluctuate based on the time of day, major events, etc.

Table 8

Hospital ER Patient Traffic Reader Potential Sizing

Size of Facility	Patient ER Traffic (Daily) Estimated	Estimated Number of Patients Seen Hourly	Reader
200	50	2	Long Distance Reader DL5510
300	75	3	Long Distance Reader DL5510
400	100	4	Long Distance Reader DL5510
500	150	6	Long Distance Reader DL5510
600	200	8	Long Distance Reader DL5510
700	250	10	Long Distance Reader DL5510
800	300	13	Long Distance Reader DL5510
900	350	15	Long Distance Reader DL5510
1000	400	17	Long Distance Reader DL5510
1100	450	19	Long Distance Reader DL5510

Reader location would be optimal either at the ER admittance desk or ER receiving locations for emergency vehicles. For both local and metro hospitals, the readers would need at

least 100M Ethernet connectivity to the application servers for transmitting the healthcare data from the readers. This network connectivity could be enough to support the initial data downloaded from the tags. Once the data is sent from the application servers to the facility patient database, it would be handled as normal IT network traffic. The data transfer from the facility database to the clearinghouse and from the clearinghouse to the insurance company database and vice versa would also be handled as normal IT network traffic.

As patients are being treated whether while in a room in the emergency department or place in a hospital RFID readers would be able to service multiple rooms based on the reader's tag reading/writing capacity, its receiving range, and the number of rooms on each floor. It is difficult to provide the RFID reader sizing for both the local and metro medical bed facilities because the square footage of the locations are not available at this time. Table 9 provides possible parings for readers to hospital floor capacity. It is also recommended that at least 2 readers be placed per floor to allow for redundancy in the case of hardware failure. Because of the readers' large tag reading capacity, they could also be used for other functions such as asset tracking or the monitoring of the patient's vital signs.

Table 9

Hospital Bedding Size to Reader Capacity

Size of Facility	Estimated Number of Readers per Floor	Reader
100	2	Long Distance Reader DL5510
200	2	Long Distance Reader DL5510
300	2	Long Distance Reader DL5510
400	2	Omni-directional Active RFID Reader
500	2	Omni-directional Active RFID Reader
600	2	Omni-directional Active RFID Reader
700	2	Omni-directional Active RFID Reader
800	2	Omni-directional Active RFID Reader
900	2	Integrated Reader
1000	2	Integrated Reader
1100	2	Integrated Reader

At this point the data in the smart tagged medical charts for each patient is uploaded from the reader through its network connection to the facility database. Both the local and metro hospitals could utilize the Long Distance Reader DL5510 reader for use in the medical charts because of the small number of tags needed to poll and write to. Also it has a smaller reading

range which is convenient for writing to the RFID wristband of the patent. As the doctors and nurse treat the patient, the information in the medical chart and wristband is updated. When the treatment is completed, the reader in the medical chart sends its data to the facility database which passes the data to the clearinghouse and goes to the patient's insurance company by way of the corporate IT network. The readers recommended in Table 9 for the hospital floor can also handle the updating of the patient's smart-tagged insurance card with the most recent data from the medical chart once the patient is discharged.

3.6.4 Intelligent ID System Tag Mapping for Identification Each RFID tag has an electronic serial number (ESN) assigned to it when it is manufactured. This ESN would be assigned to the patient data and is transmitted with the information on the tag to the RFID reader and is passed to the application servers and also to the facility database. Once data based, the ESN is used a reference point for the patient information as their medical information is updated. The RFID wristbands and medical charts would also use the ESN as a reference for the patient as they are being treated. This data is cross-referenced with the patient's medical information retrieved from the embedded RFID smart tagged insurance cards in the facility database also.

Once the patient's treatment is completed, the information in the medical chart is updated and uploaded to the facility database. When the smart tag in the insurance card is activated and polled by the RFID reader, the application server does a database lookup on the smart tag's ESN in the database. The updated medical information is then sent to the smart tag embedded in the insurance card by identifying it with the ESN. This process allows for the persons carry insurance cards to receive the correct medical information.

3.6.5 Intelligent ID System Monitoring In order to address notification of alarms for the Intelligent ID System, there are several communication areas that will need to be monitored. Table 10 displays the zones that will require monitoring for alarm reporting.

Table 10

Alarm Reporting Areas

Communication Area	Personnel to Monitor	Possible Alarms
Smart-Tagged Insurance Card  Facility Database	Medical personnel/Corporate IT	Database mismatch due to patient information
Facility Database  Clearinghouse	Corporate IT	Network connectivity
Facility Database  Insurance Company Database	Corporate IT	Database mismatch/errors
Facility Database  Medical Chart	Medical personnel/Corporate IT	Reader connectivity/tag writing errors, Information mismatch
RFID Wristband  Medical Chart	Medical personnel	Information mismatch (Patient identification/medication error)

The first area is between the smart tagged insurance cards and medical facility database. If there is a possible mismatch with the patient data on the card with what is currently in the facility database, alarms would be generated in order to catch possible fraudulent activity or possible errors in the patient data on the card or database. The second area would be between the communication link between the facility database and the clearinghouse. If the link is down or intermittent, alarms would be generated to the corporate IT element management system for IT to troubleshoot. The third area is concerning the data stored in the facility and insurance company databases. Notifications will be generated if there is a mismatch in the data. The fourth layer is between the facility database and the medical chart. Again alarming will be created if there are connectivity issues or data mismatches. The fifth area is the concerning the medical chart and RFID wristband. If there is a discrepancy regarding the data on the wristband and chart, alarms would be generated in order to prevent improper treatment or misidentification. This system would also track who prescribed the medication or treatment, allowing for accountability on the medical professional. The last area is between the smart tagged card and medical charts during the patient release from the facility. Again if there is a mismatch between the patient data on the insurance card and medical chart, alarms would be generated to allow for further investigation into the matter.

The alarms would be sent to the application servers who could forward the alarms to the medical facility IT Element Management System (EMS) or a Management System specifically for the Intelligent ID system. Using a separate management system allows the medical staff to be notified quickly when there are alarms to be addressed since they would be the personnel monitoring the mismatch alarms. This would cut down on the time to correct the issues identified by the system. It would be cost effective to use the existing IT EMS and add the RFID alarms to

be displayed. However the amount of alarms could be too much for the system and too many for the IT personnel to monitor. Also there could be possible delays in getting the notifications to the medical personnel.

3.6.6 Intelligent ID System Programming. For programming to support the Intelligent ID system, there are several programming languages already being used to support RFID technology such as Java, C, C++, and .NET. Table 10 shows the programming languages that the readers used in the previous section support.

Table 11

Programming Languages Supported by RFID Readers

(Modified from Sources: http://www.alibaba.com, http://www.rfidinfotek.com, and http://www.atlasrfidstore.com [75] [76] [77])

Reader	Manufacturer	Programming Languages Supported
Long Distance Reader DL5510	Unknown	Unknown
Omni-directional Active RFID Reader	Aerospace Innotech	C++ and C
Integrated Reader	ThingMagic	Java, C, .NET - Host C-API Reader
M6 UHF RFID Reader (4 Port)	ThingMagic	Java, C, .NET - Host MercuryOS C-API Reader
Enterprise RFID Reader	Alien	SDKJava and .NET APIs

We recommend using object oriented programming for the Intelligent ID framework. This type of programming can potentially provide the support needed for the mobile RFID environment such as our system. Object-oriented programming gives you the ability to scale because of the relatively small size of objects and the ability to manage those objects in commercially available software. It also Carreton et al (2010) in their work “Distributed Object-Oriented Programming with RFID Technology” recommend adding a natural extension to

distributed object-oriented programming by setting physical objects tagged with writable RFID tags as true mutable software objects [61][63].

Carreton et al (2010) also suggest several requirements for their model to be applied to the RFID environment [61].

- Physical objects must be addressed – In order to link software object to a physical object, a single physical object must be addressed.
- RFID tags must be able to store application data – RFID tags must be able to store data in writable memory.
- Must be able to react to objects that appear and disappear – It is essential that the programming have the ability to recognize when tags are connecting, reconnecting, and disconnecting so that the proxy objects are synchronized with the physical objects. This is imperative so that the identity of the proxy object is kept.
- Communication must be asynchronous – the messaging with proxy objects that represent physical objects should occur asynchronously so that latency is hidden and the applications respond properly.
- Communication must be fault-tolerant – Communication faults should be seen as normal instead of the exception. This permits applications to work regardless of when there are communication issues with the physical objects.

An object-oriented programming language suitable for the Intelligent ID System could possibly be Ambient-Oriented programming (AmbientTalk). It is a programming model for peer-to-peer mobile applications and takes into account the network failures that are characteristic of mobile ad hoc networks [62] [63]. It also does not require programmers to have to manually

change scripting languages and lessens the probability of programming errors due to manual intervention.

AmbientTalk has several attributes that can make it useful in the Intelligent RFID ID system. One of its attributes is that it uses a classless object model. This means that if a class is modified, there is no problem associated with it. When there is a change on a class in object-oriented programming, there have to be manual changes made by the programmer on all classes and cases of relations. This can be problematic and too difficult to resolve. Another attribute is the usage of non-blocking communication primitives. When communication is blocked, a program has to pause in order to wait for the response to a remote command whenever communication is not available. Non-blocking primitives allows the sending process to keep working while waiting on the response from the remote command [62] [63]. The last attribute is dynamic device discovery. This allows AmbientTalk to handle a mobile network topology that is consistently changing without having a need for URLs or any other kind network addressing.

Because it has built-in object creation, Ambient-orient programming allow for peer-to-peer communication and exposure of objects to other popular programming languages such as Java and .NET. This exposure allows for the consumption of industry standard cloud service providers of data.

Figure 4 is an example of how it would work in the Intelligent RFID system. Once the RFID reader polls the RFID smart tag over a peer-to-peer network, AmbientTalk objects (objects would contain patient data, insurance coverage info, etc.) are transmitted to the reader that stores AmbientTalk handler methods. Those methods then allow the transmission of AmbientTalk objects from the reader to the healthcare facility private cloud or application servers. Once exposed the object now has the ability to be managed and searched by any data elements in the

cloud or application server. This enables the retrieval of medical records such as previous history, recent treatment, and medication information. As this information is consolidated, it can be used to create a plan of treatment or diagnosis of current symptoms. The same process would work for the smart tags embedded in the patient wristbands and tag/readers in the medical charts. AmbientTalk objects (objects would contain patient data, current treatment, prescribed medication, etc.) are transmitted to the reader in the medical chart that stores AmbientTalk handler methods. Again AmbientTalk objects are sent from the reader in the medical charts to the healthcare facility private cloud or application servers to be updated and managed. This data would be available would then be updated for the smart tags in the insurance card once treatment is completed. Because of the flexibility of this programming language, it can potentially provide a viable solution for the mobility needs of the Intelligent ID System.

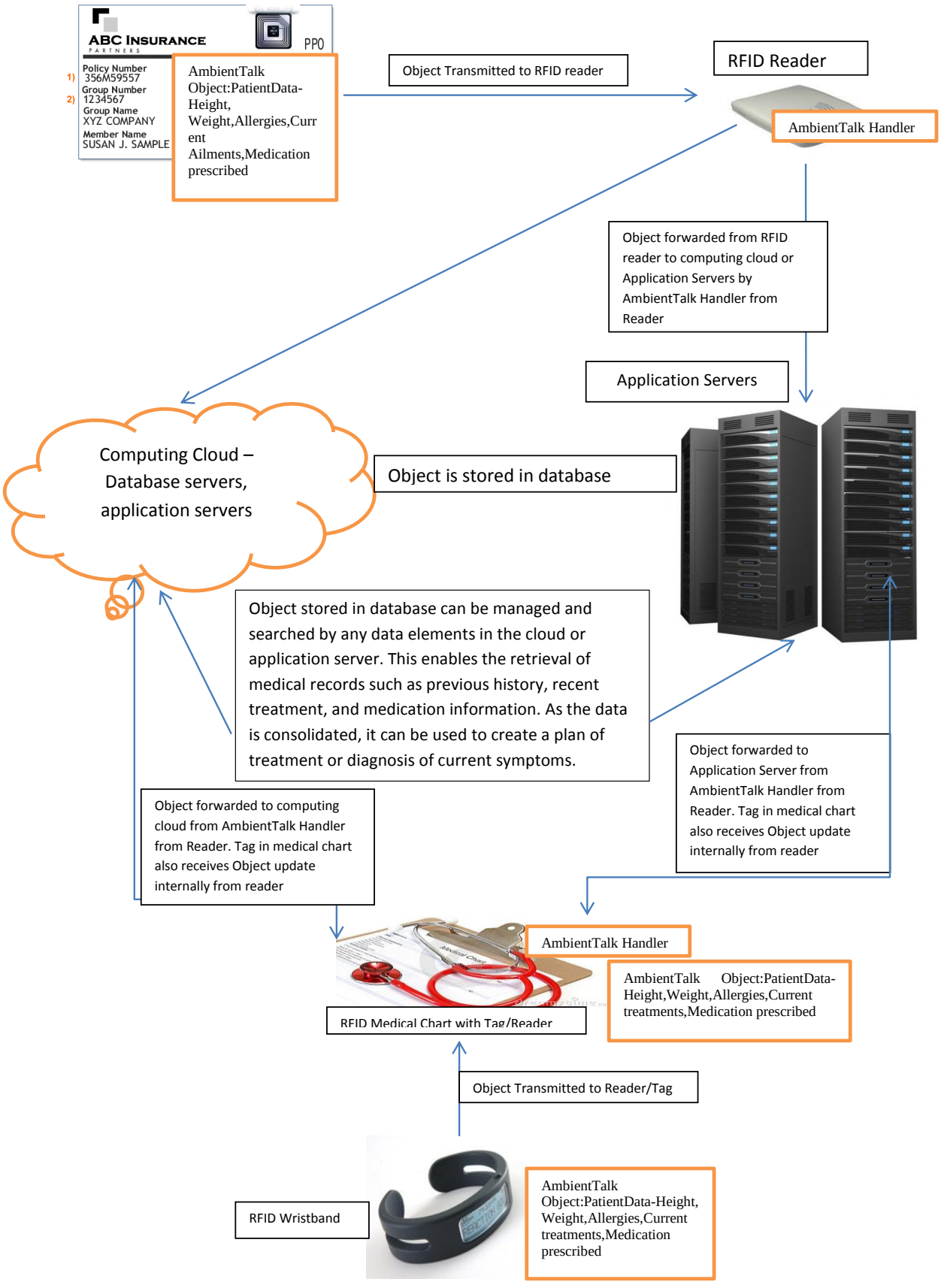
ABC INSURANCE
PARTNERS
PPO
1) Policy Number 356M59557
2) Group Number 1234567
Group Name XYZ COMPANY
Member Name SUSAN J. SAMPLE
AmbientTalk Object:PatientData-Height, Weight,Allergies,Current Ailments,Medication prescribed
Object Transmitted to RFID reader
RFID Reader
AmbientTalk Handler
Object forwarded from RFID reader to computing cloud or Application Servers by AmbientTalk Handler from Reader
Application Servers
Computing Cloud – Database servers, application servers
Object is stored in database
Object stored in database can be managed and searched by any data elements in the cloud or application server. This enables the retrieval of medical records such as previous history, recent treatment, and medication information. As the data is consolidated, it can be used to create a plan of treatment or diagnosis of current symptoms.
Object forwarded to computing cloud from AmbientTalk Handler from Reader. Tag in medical chart also receives Object update internally from reader
Object forwarded to Application Server from AmbientTalk Handler from Reader. Tag in medical chart also receives Object update internally from reader
AmbientTalk Handler
AmbientTalk Object:PatientData-Height,Weight,Allergies,Current treatments,Medication prescribed
RFID Medical Chart with Tag/Reader
Object Transmitted to Reader/Tag
RFID Wristband
AmbientTalk Object:PatientData-Height, Weight,Allergies,Current treatments,Medication prescribed

Figure 4. Ambient-oriented programming framework

3.6.7 Possible Shortcomings of the Intelligent ID System However, there can also be a number of disadvantages that this system could have. The first disadvantage is the cost of implementing it. Even though RFID tag and reader costs are decreasing, the RFID Intelligent ID solution would require every insurance card and medical chart in health care facilities to be embedded with RFID smart tags. RFID reader will need to be installed in various health care locations. Also, the IT infrastructure of the facilities along with the insurance companies will need to be upgraded and have network connectivity between each other in order for there to be seamless data flow. The initial cost to put into this operation could be difficult and would be challenging to companies willing to implement this system. The last disadvantage is providing security for the Intelligent ID system. The IT network for this system follows normal security practices for protection; however there is no definitive solution for secure communication between the RFID tag and reader. Some may consider this the most vulnerable part of RFID technology but in the following chapter, RFID security will be examined, as well as a solution we have developed for secure communication between the tag and reader.

3.7 Use of Existing Methods

The Smart Tagged Intelligent ID System components have been either proposed or are currently used in the healthcare industry. This section will review how similar technology is being utilized in healthcare facilities and its impact.

3.7.1 RFID Wristband In 1999 Walter Mosher received a patent from the U.S. Patent Office for the Laminated Radio Frequency Identification Device [27]. This device is a RFID wristband that contained laminae that covered the RFID tag components and was designed to identify hospital patients. RFID readers are linked to the RFID tag in the wristband and the

reader polls the tag for patient identification. This device is one of the crucial elements that have been implemented in hospitals to prevent patient misidentification.

The RFID wristband technology is being currently used in several hospitals such as New York's Jacobi Medical Center, in the UK Birmingham Heartlands Hospital, and in Germany the Saarbrucken Clinic Winterberg [28]. These medical facilities assign admitted patients a RFID wristband that has a passive RFID chip. The chip contains the patient's generated unique ID number and important medical data such as blood type and allergies, so that treatment can be obtained in a quicker manner. Any other private information is kept on a secure database that uses the unique ID number as a means to link with the stored data. In order to retrieve information from the wristband, a handheld computer with a RFID reader is used to scan the encrypted data. The medical personnel can access the patient's private medical information over the hospital's local area network (LAN). If the patient wants to look at their records, they can scan their wristbands by the RFID readers.

New York's Jacobi Medical Center has expanded their use of this RFID system for its blood bank. When blood is shipped to the hospital, it is assigned a RFID label that contains a chip that has enough memory to hold a unique ID number and blood type information. This number is also kept on a secured database that has the information regarding the originating location of the blood, why it is there, when assigned, and the intended patient. As the blood is prepared for transfusion, the hospital worker uses the RFID reader in the handheld computer to poll the tag on the blood and the patient wristband. If the data matches, the blood can be used for the patient. This allows for a better way to manage blood transfusions.

The UK's Birmingham Heartlands Hospital utilizes RFID technology in the operating room to make certain that the right patient is receiving surgery as it pertains to ear, nose, and

throat. The patients receive a RFID wristband that contains their information and a digital photo. The doctors use this data to verify that they have the right patient and are performing the correct procedure. If the wrong person is brought into the surgery, the team is alerted of the problem.

3.7.2 Existing Hospital Patient Management Systems. In the previous section, the use of the RFID wristband was reviewed. Hospital Patient Management Systems (HPMS) utilizing RFID have been developed which integrate the smart tags and IT systems into one. This allows the integration of the RFID wristband, RFID readers (in handheld PDAs), wireless networks, and backend database servers. This integrated system ensures that patients are correctly identified and receive the correct medical treatment [29]. It can also link other hospital databases together in case patients are transferred between locations or have had previous medical treatment that needed to be retrieved. There are six layers that comprise the RFID healthcare system architecture for HPMS.

Table 12

IT Layers for RFID-based Healthcare Systems

(Source: RFID-based Hospital Real-time Patient Management System [29]*)*

Layer	**Device/Application**
Physical	RFID hardware (Tag, Antenna, and Readers)
Middleware	Interface between the RFID reader and hospital database and patient management system
Process	Allows for data mapping, formatting, business rule implementation, and database communication
Data	Contains the Relational Database Management system and applications that the healthcare system can use to create RFID actions. Supports high volumes of RFID data and allows for customized views
Application	Interaction of multiple patients RFID wristbands in the application
User	GUI to allow the RFID tags and readers to work in a user-friendly way.

The system basically works in this manner. The RFID tags in the wristband send a unique ID number that the HPMS uses as an input to the data that is kept on the database backend. The

system keeps a record of all IDs and when information is needed, the healthcare provider only needs to select the ID and the medical information is retrieved for the patient. Unused tags can be assigned to patients throughout the system and can be unassigned once the patient has completed treatment or moved to another facility. Hospitals are adopting the use of RFID-based applications like this to increase productivity and efficiency.

Exavera Technologies has created the eShephard system that uses both RFID and Wi-Fi to track patients and workers in a healthcare facility [24]. Both technologies have been integrated into one system. The eShephard unit is connected to the facility's LAN by way of the main router. It can also route traditional voice calls over the network. It is currently being trialed in two hospitals in New England.

American Project Services in Memphis, TN is working with the University of Memphis and the Shelby County Regional Medical Center's ER to implement a RFID system to track patients. Patients had RFID tags assigned when they were admitted into the location, and was trialed with 100% accuracy thus corroborating the RFID system's effectiveness.

3.8 Summary of Existing Methods

After reviewing the data on the RFID-based technology similar to the Intelligent ID System, it is clear to see that hospitals are using the existing technology of RFID. Wristbands, readers and database systems are being used for patient identification and to make certain of proper treatment. However it appears that a comprehensive system does not exist where the patient's medical information and treatment history were kept outside of the healthcare facility and could be available if the patient had to be readmitted. A comprehensive framework that is comparable to what the Intelligent ID System provides currently does not exist. Our developmental system extends beyond the existing HPMS with the Smart-Tagged insurance

cards that allows a faster retrieval of patient medical information, which provides more efficency.

CHAPTER 4

RFID Security

4.1 RFID Security

Zhang et al (2010) stated that RFID devices are projected to become the largest number of communication devices in computing environments for applications from retail to healthcare organizations [43]. In spite of all the benefits that RFID can provide to industry, there are some security concerns that come with its use. When it comes to the security of RFID technology, the overall system design is the main factor for the general security. If the supporting systems are not protected properly, RFID suffers from the same threats as any other network technology. One of the common weak points in RFID technology is the link between the tag and reader. Usually there is no encryption for the messaging for this communication link.

The following services are provided when security methods are in place in a RFID system [43].

- Verification for the authorized communicating devices
- Privacy that stops unauthorized release of data
- Reliability of detection of any data changes
- Prevention of unapproved use of resources
- Ability to show evidence against the false denial of messaging content
- Exposure of possible threats and investigation of security breaches by logging and auditing

These services ensure the success of protecting RFID technology from security threats.

4.1.1 RFID Security Threats. The security threats to RFID technology can be put into several classes; Sniffing (or Eavesdropping), Spoofing, Cloning, Replay, Relay and Denial of

service attacks [30]. This section will review the classes of security threats and how they impact RFID networks.

The security threat that brings the highest level of risk to a RFID network is sniffing or eavesdropping attacks. Since RFID is a wireless network, it faces the same security problems of any other wireless network [33] [43]. Any type of equipment that has the ability to be on the same range of transmission as the tag and reader can access the communication link between the two. Because of the availability of electrical equipment, anyone with the right know-how can build a receiver that can capture the data communication. There are two types of sniffing attacks; passive or active. A passive attack involves a receiver that is on the same frequency of the tag and reader. The receiver has to be close to the tag in order to capture the data. This type of attack can capture the data sent from the tag and the messaging from the reader to poll the tag. The active attack is more complex and requires a transmitter and a receiver that is on the same frequency as the tag and reader. Also the initiator of the attack has to have knowledge of how the reader and tag communicate. For the active attack, the attacker does not have to be close to the RFID reader to capture data. Their equipment only needs to be close to where there are RFID tags and then poll the tags for their data.

Spoofing attacks have the ability to code tags that are blank with what appears to be legitimate data so that they are seen as valid tags. The data being used to program the blank tags could be retrieved in a sniffing attack. Tag cloning is another form of spoofing. This involves the ability to clone a valid tag to steal or obtain access in unauthorized locations. An example of this is when researchers at John Hopkins University cloned a working tag and used the cloned tag to purchase gas and opened a locked car [33].

Attacks that have a combination of sniffing and spoofing are called replay attacks. In replay attacks, the RFID tag is polled and the data from the tag is secured by the attacker. The data is then sent at a later time. Attacks like this can been seen where authentication by the RFID tag is employed where an access card is needed for facility access.

Relay attacks utilize two devices: the ghost and the leech. Peris-Lopez et al in the article "Attacking RFID Systems" provide the description and process of how the relay attacks operate on a RFID system [34]. The ghost device counterfeits as a tag to the RFID reader and the leech imitates the reader to the card. A data communication link is generated by the ghost and leech to the valid reader.

1. The valid reader sends message (A) to the ghost.
2. The ghost takes delivery of the message (A) and forwards it to the leech by the data communication link with no or minimum delay.
3. The leech imitates the valid reader and transmits message (A) to the valid tag.
4. The valid tag compiles a new message (B) and sends it to the leech.
5. The leech accepts the message (B) and transmits it to the ghost by the data communication link.
6. The ghost sends message (B) to the valid reader.

The relay attack does not require that the tag and reader have to be in close proximity to each other for communication. Also encrypted messaging is not immune to this type of attack since the messaging is still being relayed through the data communication link with minimal delay with no need of knowing the content of the encrypted messaging.

The last type of threat is the denial of service attack. This type of attack is against the accessibility of the RFID system and can hit any portion of the system (reader, tag, and backend

computers). One of the ways this attack is used is when thieves remove the RFID tag from merchandise before it comes in the area of the reader. Another form is when tags are swapped and placed on merchandise that has a lower cost. This can impact database integrity on the backend systems because of the inventory mismatches.

4.2 RFID Security Countermeasures

There are several methods being used as countermeasures to the security threats presented against RFID technology. These methods can be categorized into two groups; non-cryptographic systems and cryptographic algorithms [32].

4.2.1 Non-Cryptographic Methods. In order to diminish costs non-cryptographic security countermeasures can be used. These measures can be categorized into several methods; Faraday cages, Tag commands (Kill and Sleep), selective blocker tags, and rewritable memory.

A low-technical way of providing RFID security is through the use of Faraday cages. Faraday cages are also called meshes and are used as covers for tags or smart-tagged cards such as passports. These covers are made up of metals that are manufactured in a design that create a barrier to radio waves. This prevents the tags from being read while they are covered in the Faraday cage. The tag must be uncovered when it needs to be used and the cage does not provide protection while the tag is out of the cover [34].

One of the easiest ways to safeguard consumer privacy is tag-killing [30]. This method kills the functionality of the RFID tag once it is at the point of sale. The Kill command is built into the RFID tag and is executed once the RFID reader sends a code or PIN at the point of sale to make the tag unusable. The problems with this solution are that this command does not work until it is implemented and needs to have another security function added with it to have

protection for the tag until the command is turned on. Also the tag is made unusable once the kill command is executed [34].

Because the kill command makes the tag unusable after it is carried out, a variation of the kill command was created called the sleep command. This command temporarily deactivates the tag until it is physically reactivated. Also the tag cannot be turned back on by radio signals from another reader [15].

Another method is using blocker tags. Blocker tags replicate the RFID tags serial ID numbers in a particular zone or area and can provide selective protection for the zone from being read by outside parties [36].

Utilizing the tags read-writable memory is another way of providing protection [37]. This scheme uses a secret and temporary ID code in the RFID tag's RAM and the tag's serial ID number that is created by the manufacturer and installed in the tag's ROM. The result is when the tag is in ROM mode object there is unrestricted object identification to whichever user that needs information and when in RAM mode, there is a restriction of object identification to limited users.

4.2.2 Cryptographic Algorithms. Cryptographic algorithms are more costly to implement but can provide better security and privacy. Several methods will be reviewed in this section. Those methods are Hash Based Access Control, Minimalist, Re-encryption scheme and universal re-encryption, and Advanced Semi-Randomized Access Control (A-SRAC) [35].

Hash Based Access Control uses hash-enabled tags that have a segment of memory set aside for a temporary MetaID. This allows the tag to function in a locked or unlocked status. In order to lock a tag, the hash of an indiscriminate key is kept as the tag's MetaID. When the tag is locked it will only reply to any poll for data with its MetaID. If the tag needs to be unlocked, it

has to be polled internally by its MetaID. Then there is a database search on the local database for the corresponding hash key and it is sent to the tag. The tag receives the hash key and checks it against the MetaID. If it corresponds, the tag unlocks and allows full data retrieval to the readers. This method can be expensive and is open to Denial of Service attacks.

The Minimalist method uses a list of pseudonyms that is unique to the keys stored in the RFID tag [38]. The reader is validated after it has been authenticated by the tag. It is then validated by the reader by sending an authentication key. Once the validation process is complete, the RFID tag releases its data to the reader. Then the reader renews the pseudonym and authentication keys in the tag. This prevents DOS and eavesdropping attacks. Minimalist; however, require more tag memory for storage.

Re-encryption and universal re-encryption systems use public key cryptographic methods and require more memory and server resources on the backend due to the type of algorithms being employed [35]. They can keep the tag identifier from being disclosed by utilizing the re-encryption system.

The A-SRAC algorithm employs minimal calculations and keeps the messaging size small [35]. This allows for optimal execution of the algorithm. The backend servers keep the old and new data from the tags, which prohibit DOS attacks. The A-SRAC algorithm employs hash functionality, a random generator, and also utilizes MetaID to stop tag tracking. The algorithm works in this fashion. The RFID reader queries and sends a random number to the tag. The tag sends a MetaID (which includes a random number, and hash key) to the reader, and forwards the response to the server. The server performs a database lookup on the key using the MetaID, generates a random number, and verifies if the hash key and random number are different from the other MetaIDs. If it is not, then the server renews its random number until the hash key

becomes exclusive. Then server checks to see if the random number and hash key are correct. If it is then the server sends its response back to the tag through the reader and the tag verifies if the response is correct. If it is correct then the tag sends its data to the RFID reader.

4.3 Security Framework for Smart Tags

We suggest using the A-SRAC protocol to provide security for RFID smart tagged cards with the feature to go to sleep when the smart tags do not need to transfer data and biometric verification to activate the card. The tag embedded in the card will have folders that will hold personal identification information, medical records, dental records, and other related information. The A-SRAC protocol offers a random generator and hash functionality which is two layers of security [39]. It also reduces the overhead computing resources of the server and reader. The sleep command is a variation of the kill command, where the reader transmits an access code to deactivate the tag. The tag is turned on by biometric verification. The owner's fingerprint or other physical attributes digital image is uploaded to the smart tag on the card and it is turned on when the card owner matches the fingerprint or physical attribute with the information that is on the backend servers. Using A-SRAC, the sleep command, and biometric verification will require a smart tag with sufficient memory and processing power. On the backend there must be enough server resources for security and transactions to take place.

Figure 5 shows the security process for the RFID intelligent ID system.

1. Once a patient enters a healthcare facility with his insurance card, the card is activated by biometric verification, and the reader sends a query and random number to the card.
2. The card uses the hash function to create a MetaID with an embedded key and sends it to the RFID reader.

3. The reader sends the information to the server and it performs a database lookup on the key response for the MetaID, creates a random response number and checks if the combination is unique from the stored MetaIDs. If it is not, the server renews the random number until the combination becomes unique.
4. The server updates the key and sends the information to the reader which forwards the information to the tag.

   The tag validates the information and if valid, it updates the data and releases the patient's health data from the card to the tag.
5. The reader sends an access code to the smart tag in the card to deactivate it.
6. As the patient is being treated the data that was transferred from the tag is transferred to an electronic health chart that has an embedded tag/reader in it using the same process in steps 2 – 5.
7. The health chart is updated by the medical professionals and once the treatment is completed, the card is activated by a biometric validation and goes through steps 2 - 5.
8. The reader in the health chart updates the tag in the insurance card with updated medical data and issues the access code to deactivate the card, completing the process.

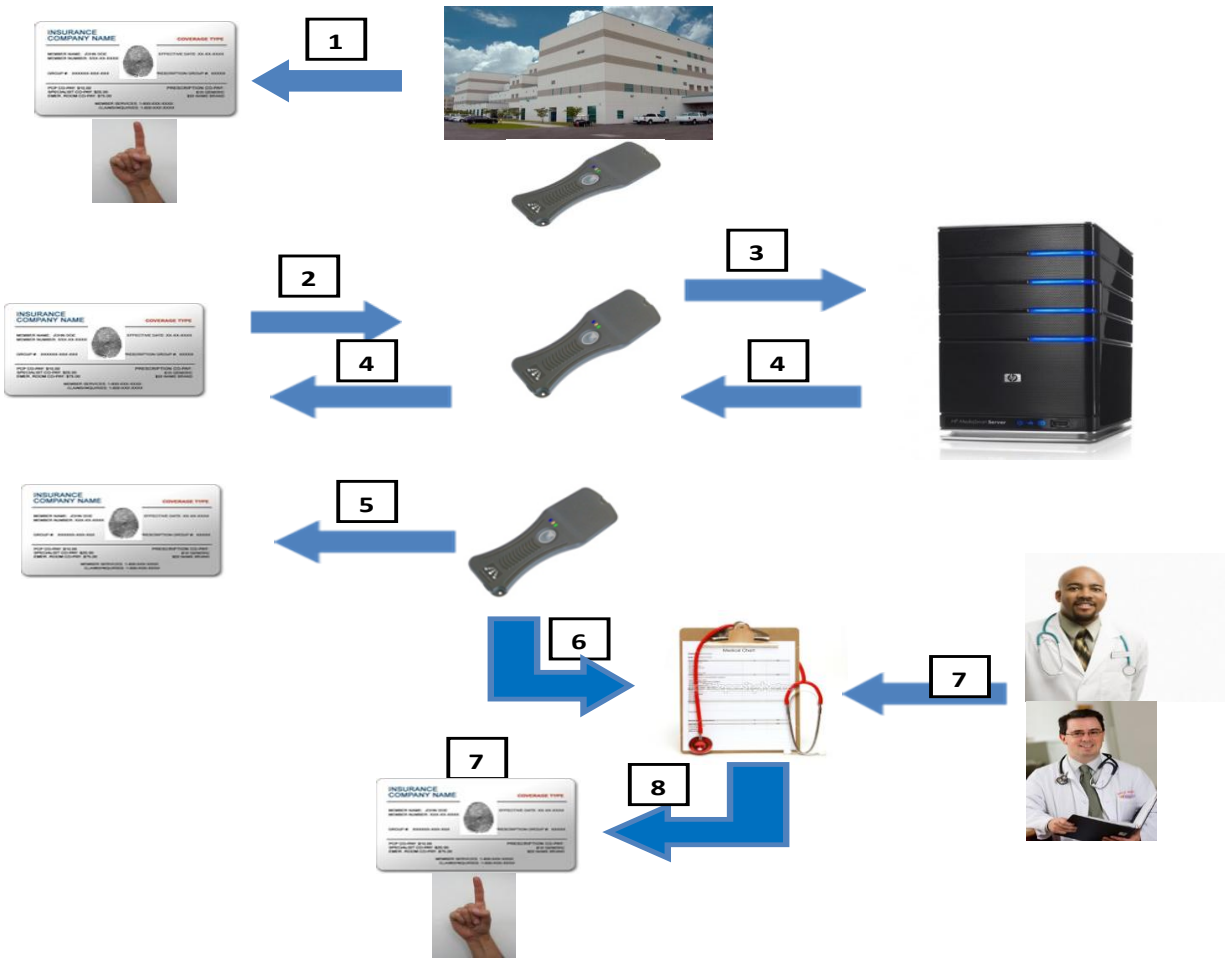

Figure 5. Proposed RFID Smart Tag Security Process Flow

4.3.1 Intelligent ID Security Framework Operational Description In this section we will examine the hospital sizing to reader capacity for the Intelligent ID security framework. The same hospital ER traffic and bed sizing models used in section 3.6.3 will be utilized. As noted earlier in section 3.6.3, the average number of daily ER patient traffic for the local and metro hospitals is similar. This data will be used again for our analysis.

Table 13 denotes the type of reader needed to support the patient ER traffic based on the different facility sizes. Because of the reader tag reading capacity, the type of RFID reader needed at the point of entry will be determined by the number of patients served by the location.

Initially the readers will query the smart tags in the insurance cards after the tags are activated biometrically and send a random number to the card, which requires a minimal amount of internal computing resources. This does not impact the amount of RFID readers needed and is the same number that was needed in section 3.6.3. Because the security framework relies mostly on the computing power of the backend servers involved in the A-SRAC protocol, there is a nominal impact to the RFID readers. The Long Distance Reader DL5510 that can scan 30 to 50 tags per second would be more than enough to handle the traffic in either the local or metropolitan hospitals based on the average number of patients served in the ER.

Table 13

Hospital ER Patient Traffic Reader Potential Sizing

Size of Facility	Patient ER Traffic (Daily) Estimated	Estimated Number of Patients Seen Hourly	Reader
200	50	2	DL5510
300	75	3	DL5510
400	100	4	DL5510
500	150	6	DL5510
600	200	8	DL5510
700	250	10	DL5510
800	300	13	DL5510
900	350	15	DL5510
1000	400	17	DL5510
1100	450	19	DL5510

When patients are admitted to the hospital and place in a room they will be assigned a RFID wristband and a medical chart embedded with a smart tag and reader. The security process will be repeated once the smart tagged wristband and medical charts are activated for use. Table 14 shows the recommended reader to support the hospital bedding size. The same amount of readers shown in this table is the same as is noted in section 3.6.3. Again this is due to minimal amount of computing resources required by the reader to query the smart tag and transmission of

the random number to the tag. Also the A-SRAC protocol function is handled on the backend servers which should cause a minor impact to the internal resources of the reader.

Table 14

Hospital Bedding Size to Reader Capacity

Size of Facility	Estimated Number of Readers per Floor	Reader
100	2	Long Distance Reader DL5510
200	2	Long Distance Reader DL5510
300	2	Long Distance Reader DL5510
400	2	Omni-directional Active RFID Reader
500	2	Omni-directional Active RFID Reader
600	2	Omni-directional Active RFID Reader
700	2	Omni-directional Active RFID Reader
800	2	Omni-directional Active RFID Reader
900	2	Integrated Reader
1000	2	Integrated Reader
1100	2	Integrated Reader

The data in Table 14 also supports the reader to floor sizing when the patient is discharged and the security process is repeated as the patient's smart tagged insurance card is

updated with the data from the medical chart. Again this is due to the reasons noted in the previous paragraph.

4.3.2 Benefits of Using the Intelligent ID Security Framework There are several advantages to using the Intelligent ID security framework. This system allows for several layers of protecting the data on the card and the data transmission over the air interface between the tag and reader.

The first layer of protection is the biometric activation. This permits the tag to transmit data only when the card is activated biometrically and keeps the tag from sending data when the card is inactive. The card carrier does not have to worry about their medical information being hacked when carrying the inactive card.

Another layer of defense is the A-SRAC protocol which provides the security validation for the smart tag to reader data transmission. This prevents unauthorized readers from accessing the patient information on the smart tag and also prevents tag cloning. This protocol utilizes backend server resources for the validation process and requires minimal internal resources from the RFID readers.

The last layer of protection is the use of the sleep command to deactivate the smart tagged devices after it completes the data transmission process. This keeps the card from sending data when polled by a reader and also allows for a longer battery life in the smart tag.

4.3.3 Shortcomings of the Intelligent ID Security Framework The security framework is specific to the tag and reader communication layer and relies on the healthcare provider's IT infrastructure to manage security on the network equipment. This process permits two layers of security to protect the data on the smart tag, one cryptographic and the other physical. There are several possible shortcomings for the security framework solution.

One shortcoming is the effect of electrostatic discharge on the RFID tags embedded in the cards. Electrostatic discharge (ESD) is a regular occurrence in electronics and happens when an electrical current flows from an item of high potential to one with low potential [50]. ESD can damage or completely render electrical equipment useless. Bauer-Reich et al (2008) in their research "The Interaction of Electrostatic Discharge and RFID" tested the impact of ESD on RFID integrated circuits. They found that 4% of the RFID tested with ESD failed [50]. If a tag fails due to ESD, of course the security protocols would be ineffective.

Another shortcoming is the impact of electromagnetic interference (EMI) on the RFID smart tag embedded in the insurance card, on the RFID readers, and the smart tags embedded in the patient charts. If there are other medical devices that transmit on the same frequency as the RFID devices, the communication path between the smart tags and readers could be disrupted, thus also impacting the security protocols for those devices. EMI from the RFID devices can also have the same effect on medical equipment [48] [50].

The last shortcoming is having insufficient server resources on the backend to support the system. The A-SRAC algorithm requires backend servers to support the data messaging for the security algorithm. When multiple tags are requiring authentication the servers need memory and CPU resources to meet the requests. If the IT server sizing is inaccurate, the security needs will not be met effectively.

CHAPTER 5

Conclusion and Future Research

In this last chapter, we will not only share the main conclusion of this thesis, but will focus on the methodology used and also provide topics for future research. The aim is to solve the problem of medical errors using RFID and explore the potential use of the technology based on the data provided in the research for this study. In the first section, we discussed the motivation behind the study of RFID technology. Because over 98,000 patients die each year from medical mistakes that could be prevented, the goal is to provide a solution using RFID technology in the healthcare industry that will save patient lives by reducing the occurrences of patient misidentification. We provide a short outline for the proposal for a RFID system using insurance cards with embedded smart tags and RFID readers in healthcare locations. This system will assist in making sure that the patient is correctly identified, the patient receives the correct medical procedure and the patient receives the correct medication. This solution allows for the patient medical data such as blood type, allergies, and prior medical history to be stored on the smart tag. The health insurance coverage information is also included. With this information available the patient does not have to verbally provide it if they are incapacitated. The healthcare provider can correctly identify the patient and treat him or her faster. They can also update the medical information as the patient receives treatment.

For the second section, an overview of RFID technology is given along with its system components. The RFID system comprises three fundamental parts; the RFID tag, the RFID reader, and the RFID controller. The RFID tag and reader communicate with each other on a specified radio frequency. The RFID reader retrieves the data from the tag and sends the information to the RFID controller. The RFID controller takes the data and uses it based on the

type of data it has received. RFID tags can be categorized into different classes depending on the capability needed. RFID tags are active, passive, or semi-active. The RFID reader can read the data of the tag, send data to and from the RFID controller, and send power to tags that are passive. The RFID controller is the main management element in a RFID system. It provides connectivity from many RFID readers, contains the main database, and also has the system software. RFID can operate in frequency ranges from Low, High, Ultrahigh, and Microwave. The ranges depend on the use required for each system. In the healthcare industry, the frequency range of 13.56 MHz is utilized. The developments that caused the expansion of RFID technology in industry are noted. Some of the developments were protocol standardization, low pricing for RFID tags, the availability of higher frequencies, and the growth of the internet as a part of company's IT infrastructure. Commercial business will be the main area where RFID growth will be seen especially in inventory tracking. RFID manufacturers will mainly focus on technology development in areas that will increase the use of RFID components. Market expansion will be dependent on the cost to implement and maintain the technology. Some of the issues that hinder RFID growth are the high cost to implement the system, the lack of global standards, and the security/privacy issues that are associated with the technology. Future use will be seen in the home where household appliances can be monitored.

In the third section the different types of medical errors seen in the healthcare field are reviewed. Those errors are patient misidentification, inaccurate diagnosis, wrongly prescribed medication, and surgical errors. The main departments in hospitals which are the emergency room, the inpatient ward, and outpatient care are discussed. There is an assessment of the process flow between those units, along with the problems that they typically face. In the healthcare industry, we found several benefits that RFID brings to the table. These benefits are the

enhancement of patient safety, savings to time and costs, and increasing efficiency. The limitations to using the technology in healthcare are examined. These limitations involve three areas: technical, economical, and privacy/security limitations. There are several technical limitations; physical, RFID scalability, and data management. Economic limitations involve the cost companies have to pay to purchase and implement a RFID system. Privacy/Security limitations deal with the security of the RFID data. Since the RFID tags contain unique identifiers that are connected to personal information, healthcare providers must make sure that the transmission of the data is secure and cannot be pulled at random from the RFID tags. The data could be used to invade patient privacy. Our study looked at the how RIFD technology is being implemented in the healthcare industry. Some of the applications that RFID is being used in are asset tracking, identification and verification, and monitoring.

The third section also addresses the RFID intelligent ID system which has been developed to deal with the issue of medical errors. The system framework is based on RFID smart tags embedded in personal health insurance cards. Insurance cards were recommended because they are convenient to carry and people normally have them on their person whether in a wallet or purse. Smart tags were chosen because of their ability to read and write data to its memory and the storage capacity. The battery life is another reason why smart tags were chosen to be utilized in our framework. The battery technology developed now for smart tags can cause the tags to last 10 years [52]. The smart tagged cards will only transmit data when polled by the reader which assists with increasing battery life. Energy is conserved when the tag in the card is not transmitting. These tags also have a longer communication range and allows for the patient's data to be updated as they are moved through the medical facility. Because of these factors, the insurance cards with embedded tags need only to be replaced when there is a malfunction or

when the battery dies. The process in which the system would work was reviewed. The tag readers for this system have to be under government oversight and are issued to healthcare providers that are registered for its use. Smart tags are also utilized in patient wristband and patient chart. The medical data in the smart tagged card can include the following information such as; date of birth, age, height, weight, and current medical conditions. The medical conditions will show if the patient had allergies, type of medication being prescribed, current aliments, and the insurance coverage for the patient. Once the patient comes into a healthcare facility for treatment, a RFID reader retrieves the medical data from the smart tag in the insurance card and transmits the data to the facility database. The data is then transferred to the health insurance company's database through a clearinghouse or third party that translates the healthcare facility data into a format that the insurance company can process and keep in data storage. As the patient is being prepared for treatment, their medical data is uploaded to a patient chart that has a smart tag embedded in it and the patient is also fitted with a wristband embedded with a smart tag. The wristband tracks the patient's medical treatment and health condition. When the treatment is finished, the medical chart and wristband sends the updated information to the healthcare facility database and the data is also sent to the insurance company's database for billing through the clearinghouse so that the insurance company can process the updated medical data. The medical chart and wristband embedded smart tags are erased for reuse and the smart tagged insurance card is updated with the new medical data for the patient for possible future treatment. We reviewed possible design scenarios using several operational models. One model was developed by a short survey for the hospitals in Greensboro, N.C. Information was requested regarding the hospital bed capacity and estimated number of emergency room patients seen daily in the regional hospitals. Another model was created using internet research data for hospitals in

major metropolitan cities using the number of beds and estimated number of patients seen yearly. We also identified several RFID readers on the market that could be used for the Intelligent ID system and their capabilities. Based on this data, we attempted to size the reader capacity with the potential hospital traffic, using the path that the patient's medical data would take as they were treated the hospital environment. We reviewed how the readers would send the correct data to the smart tags embedded in the insurance cards and RFID wristbands. The communication will be based on the electronic serial number (ESN) assigned to tags when they are manufactured. This ESN would also be assigned to the patient data on the tag and is transmitted with the information on the tag to the RFID reader and is passed to the application servers and also to the facility database. Once data based, the ESN is used a reference point for the patient information as their medical information is updated. The medical charts would also use the ESN as a reference for the patient as they are being treated. This data is cross-referenced with the patient's medical information retrieved from the embedded RFID smart tags in the facility database also. Once the patient's treatment is completed, the information in the medical chart is updated and uploaded to the facility database. The smart tag in the insurance card is activated and when polled by the RFID reader, the application server does a database lookup on the smart tag ESN in the database. The updated medical information is then sent to the smart tag. We also developed several methods for monitoring for the Intelligent ID system. There were several layers identified for monitoring alarms. The first layer was the information between the smart tagged insurance card and medical facility database. If there is a possible mismatch with the patient data on the card with what is currently in the facility database, alarms would be generated in order to catch possible fraudulent activity or possible errors in the patient data on the card or database. The second area would be between the communication link between the facility

database and the clearinghouse. If the link is down or intermittent, alarms would be generated to the corporate IT element management system for IT to troubleshoot. The third area is concerning the data stored in the facility and insurance company databases. Notifications will be generated if there is a mismatch in the data. The fourth layer is between the facility database and the medical chart. Again alarming will be created if there are connectivity issues or data mismatches. The fifth area is the concerning the medical chart and RFID wristband. If there is a discrepancy regarding the data on the wristband and chart, alarms would be generated in order to prevent improper treatment or misidentification. This system would also track who prescribed the medication or treatment, allowing for accountability on the medical professional. The last area is between the smart tagged card and medical charts during the patient release from the facility. Again if there is a mismatch between the patient data on the insurance card and medical chart, alarms would be generated to allow for further investigation into the matter. The alarms would be sent to the application servers who would forward them to the IT Element Management System (EMS) or a Management System designed specifically from the Intelligent ID system. We reviewed the advantages and disadvantages of using a management system designed for the Intelligent ID system. Advantages were using the medical staff to monitor the system and causing them to be notified quickly when there were alarms to be addressed. A disadvantage was the cost to implement such a system. The advantages and disadvantages of using the existing EMS were also discussed. It was cost effective to use the existing IT EMS and add the RFID alarms to be displayed. However the amount of alarms could be too much for the system and too many for the IT personnel to monitor. Also there could be possible delays in getting the notifications to the medical personnel.

Furthermore in the third section, we also discussed the type of programming needed for the Intelligent ID System and noted the different programs being used for RFID readers on the market. Our recommendation was to use object-oriented programming because it potentially provides the support needed for the mobile RFID environment. Object-oriented programming gives us the ability to scale because of the relatively small size of objects and the ability to manage those objects in commercially available software. One of these types of programming languages we looked as a possibility to support our system was Ambient-Oriented programming (AmbientTalk). This was because it is a programming model for peer-to-peer mobile applications and takes into account the network failures that are characteristic of mobile ad hoc networks [62]. It also allows for peer-to-peer communication and exposure of objects to other popular programming languages such as Java and .NET. We allow reviewed how it could work in the Intelligent RFID system. Once the RFID reader polls the RFID smart tag over a peer-to-peer network, AmbientTalk objects (objects would contain patient data, insurance coverage info, etc.) are transmitted to the reader that stores AmbientTalk handler methods. Those methods then allow the exposure of AmbientTalk objects to healthcare facility private cloud or application servers. Once exposed the object now has the ability to be managed and searched by any data elements in the cloud or application server. This enables the retrieval of medical records such as previous history, recent treatment, and medication information. As this information is consolidated, it can be used to create a plan of treatment or diagnosis of current symptoms. Similar RFID-based technology was reviewed to see if our system had already been implemented. RFID tagged wristbands and readers are starting to be used in healthcare facilities for patient identification and to verify that they are receiving the correct treatment. RFID-based Hospital Patient Management Systems have integrated the RFID tags, readers, and wireless

networks into a single system. The issue is that neither solution extends outside the hospital nor resolves the issue of not having the availability of the patient's medical data in case of an emergency or if the patient needs to be treated for a different issue.

The fourth section deals with RFID security. In this section, we discuss the security threats facing RFID technology. The overall system design is the main factor for general security. When the supporting systems are not protected properly, RFID systems can suffer the same threat as any other network technology. The common weak point in RFID technology is the interface between the tag and the reader because there is no encryption for the messaging on this communication link. RFID security threats are discussed. Several of the security threats reviewed were; sniffing (eavesdropping), spoofing, cloning, and denial of service attacks. RFID security countermeasures were reviewed and are broken down into two categories; Non-Cryptographic and Cryptographic. Non-Cryptographic include these methods; Faraday cages, Tag Commands (Kill and Sleep), Selective Blocker tags and rewritable memory. Cryptographic algorithms are more expensive to implement but provide better security and privacy. Several cryptographic algorithms reviewed were; Hash Based Access Control, Minimalist, and Advanced Semi-Randomized Access Control (A-SRAC).

For the RFID smart tagged insurance card system we developed a security framework for the RFID Intelligent ID system. There are three types of security methods recommended. The card is activated to transmit data by biometric verification and the A-SRAC protocol is used to validate that the smart tag embedded in the insurance card is authorized to transmit data to the tag reader. Once the data is transmitted to the reader, the reader sends a code to the tag to sleep into until biometric verification activates the tag again. This process is repeated also before the reader transmits data to the smart tag embedded medical chart and again to the insurance card as

the patient is discharged from the medical facility. There was a review for possible design scenarios for the Intelligent ID security framework using the models developed in Chapter 3. It appeared that the same design models could be applied to the security framework due to minimal impact to the internal resources of RFID readers of the protocols recommended in our security framework. We also reviewed the advantages of using the security framework. One advantage is that the smart tagged cards will not transmit data when it not activated biometrically. Another advantage is that the use of the A-SRAC protocol keeps unauthorized readers from retrieving patient data on the rags and also prevents tag cloning. The use of the sleep command created the last advantage of the security framework. The smart tagged card is rendered inactive after it completes the data transmission to the reader and allow permits longer battery life for the smart tag. Several possible shortcomings were identified with the security framework: effect of electrostatic discharge (ESD), electromagnetic interference (EMI), and backend server resources.

5.1 Contributions

The following are the main research contributions of this thesis;

- An intelligent RFID smart tag framework was developed to prevent medical errors by ensuring patient identification and that patients receive the proper medication. This framework is theoretical and provides a direction for future research.
- Ambient-oriented programming (Object-oriented programming) was recommended as a programming solution to support the mobile RFID environment for the Intelligent ID system. Additional study is needed to validate the use of this programming language.
- Adding cloud computing to the Intelligent RFID framework was recommended to add more computing resources to the system in order to address RFID scalability.

- Developed a solution connect the smart tag's electronic serial number (ESN) to the patient information on the tag in order to ensure that the data was tracked and uploaded to the correct smart tagged insurance cards and RFID wristbands. This is an opportunity for more research.
- A security solution has also been developed to cover the tag to reader air interface. The solution uses A-SRAC, biometrics, and the sleep command to prevent the tag from transmitting data when it is not needed. Further research is needed in this area to prove that the smart tags can support the security framework.

5.2 Future Research

The framework provided in this thesis presents a normal guide to future research. The RFID Intelligent system framework establishes a comprehensive system that will greatly benefit healthcare facilities. This creates research opportunities for each of the system components. One of the areas is the storage capabilities of smart tags. Smart tag development has resulted in greater storage capacity on the tags. Higher capacity tags can support theoretically up to 216 KB and can store large data strings (Pais & Symonds, 2011). This could allow for projects to validate tag storage capacity for biometric and patient medical data. Also further study could be used to develop the data strings for the patient's medical data that is to be stored on the tags embedded in insurance cards. Another area for research is the database development needed to support a clearinghouse that will translate the healthcare facility data to formats supported by insurance companies. Testing Ambient-oriented programming for the patient medical data needs to be validated. Also correlating the smart tag electronic serial number to patient data would be an additional research opportunity.

For the smart tag security aspect, there are opportunities for future study to verify that the security protocols suggested for the system framework can support the smart tags effectively. The A-SRAC protocol can be an effective means for authentication security. Further research would be needed to verify that the RFID readers can effectively shut down tag transmissions with the sleep command. Proper CPU and memory resources requirements will need to be designed for the back-end servers to support the security protocols.

Future studies should be able to validate the RFID Intelligent ID System and the requirements of its components. This framework produces opportunities for research to confirm the smart tag capability for biometrics, patient data storage, and ESN use for patient data correlation. Research development is needed for ambient-oriented programming in the Intelligent RFID system. Opportunities for future development are a must for the security for the air interface between the RFID tag and reader to adequately ensure that patient data is protected and is not vulnerable to hacking.

References

1. K.A. Stroetmann, T. Jones, A. Dobrev and V.N. Stroetmann, "eHealth is worth it – The economic benefits of implemented eHealth solutions at ten European sites", European Commission, Luxembourg: Official Publications of the European Communities (OPOCE), 2006.
2. S.J. Kim and N.-S. Kim, "An approach about Implementation and Use of One-Stop Healthcare Service System Using RFID Technology", in proceedings ICACT 2006, pp. 339-344
3. J. Halamka, "Early experiences with positive patient identification," Journal of Healthcare Information Management, Vol. 20(1), p.p. 2027, 2006
4. Wang, S., Chen, W., Ong, C., Liu, L., Chuang, Y., 2006. RFID applications in hospitals: a case study on a demonstration RFID project in a Taiwan hospital. In: Proceedings of the 39th Hawaii International Conference on System Sciences. pp. 184
5. Hunt, V., Puglia, A., & Puglia, M. (2007). *Rfid-a guide to radio frequency identification*. Hoboken, NJ: John Wiley & Sons, Inc.

   RFID Adoption and Implications A Sectoral e-Business Watch study by IDC / Global Retail Insights Final Report. (2008, September). *http://www.empirica.com*. Retrieved February 20, 2013, from http://www.empirica.com/themen/ebusiness/documents/Study_07-2008_RFID.pdf
6. Kuo, C., & Chen, H. (2008, January). *The critical issues about deploying rfid in healthcare industry*. Retrieved from http://www.computer.org/csdl/proceedings/hicss/2008/3075/00/30750111-abs.html

7. Forsloff, C. (2010). Impact of wrong diagnosis on health care in america . Retrieved from http://digitaljournal.com/article/287533
8. Harrop, P. and Das, R. (2006) 'RFID in Healthcare 2006 – 2016: report summary'. IDTechEx.
9. Kohn, L. T., Corrigan, J., Donaldson, M. S. K., Corrigan, J., & Donaldson, M. S. (1999). Retrieved from http://www.iom.edu/Reports/1999/To-Err-is-Human-Building-A-Safer-Health-System.aspx
10. Aguilar, A., Putten, W. V. D., & Maguire, G. (2006). *Positive patient identification using rfid and wireless networks*. , Dublin, Ireland. doi: web.it.kth.se/~maguire/../070323-Antonio-Aguilar-with-cover.pdf
11. IDTechEx. (2006). *Rapid adoption of rfid in healthcare*. Retrieved from http://www.idtechex.com/research/articles/rapid_adoption_of_rfid_in_healthcare_00000470.asp
12. O'Reilly, K.B. (2010). American Medical News - amednews.com. *Diagnostic errors: Why they happen - amednews.com.* Retrieved March 11, 2013, from http://www.amednews.com/article/20101206/profession/312069947/4/
13. Peterson, M. (2010, June 24). *100,000 americans die each year from prescription drugs, while pharma companies get rich*. Retrieved from http://www.alternet.org/story/147318/100,000_americans_die_each_year_from_prescription_drugs,_while_pharma_companies_get_rich

    Worst pills, best pills. (2012). Retrieved from http://www.worstpills.org/public/page.cfm?op_id=3

    ("Worst pills, best," 2012)

14. Torrey, T. (2011, October 26). *Why do prescription drug errors occur*. Retrieved from http://patients.about.com/od/drugsandsafety/a/prescerrors.htm

15. Banks, Jerry & Pachano, Manuel & Thompson, Les & Hanny, David. (© 2007). Rfid applied. [Books24x7 version] Available from http://0-common.books24x7.com.sheba.ncat.edu/toc.aspx?bookid=20486.

16. Lee, Cheon-Pyo, and Jung P. Shim. "Exploratory Study of Radio Frequency Identification (RFID) Adoption in the Healthcare Industry." *European Journal of Information Systems* 16 (2007): 712-14. Print.

American association for justice. (2013). Retrieved from http://www.justice.org/cps/rde/justice/hs.xsl/8677.htm

17. Yao, W., Chu, C., & Li, Z. (2010). *The use of rfid in healthcare: Benefits and barriers*. In *Program for the IEEE International Conference on RFID-Technology and Applications*. Guangzhou, China:

18. Brown, Dennis E.. (© 2007). Rfid implementation. [Books24x7 version] Available from http://0-common.books24x7.com.sheba.ncat.edu/toc.aspx?bookid=18178.

19. A. M. Wicks, J. K. Visich, and S. Li, "Radio frequency identification applications in hospital environments," *Hospital Topics*, vol. 84, pp. 3-8, 2006.

20. Figarella, L., Kikirekov, K., & Oehlmann, H. HEALTH INDUSTRY BUSINESS COMMUNICATIONS COUNCIL, (n.d.). *Radio frequency identification (rfid) in healthcare benefits, limitations, recommendations*.

21. Cho, J., Cobbs, S., Curtiss, E., Overton, K., & Redner, M. (2012). *Use if rfid in healthcare industry*. Informally published manuscript, Colorado State University, Colorado State University, Pueblo, CO, , Available from AABRI. (OC13056)Retrieved

from http://www.google.com/url?sa=t&rct=j&q=use of rfid in healthcare industry&source=web&cd=3&cad=rja&sqi=2&ved=0CEwQFjAC&url=http://www.aabri.com/OC2013Manuscripts/OC13056.pdf&ei=X2IzUdrlA5Sc9QShooGQBw&usg=AFQjCNHT-jsOwEKN7dWWoVxl3pUtDslgeA

(Cho, Cobbs, Curtiss, Overton & Redner, 2012)

22. Kalb, C. (2010, September 27). *The daily beast*. Retrieved from http://www.thedailybeast.com/newsweek/2010/09/27/how-we-can-prevent-medical-errors.html
23. Wicks, A., Visich, J., & Suhong, L. (2006). *Radio frequency identification applications in hospital environments*. DOI: pmlab.iecs.fcu.edu.tw/PP/Papers/RF/WiVL06.pdf
24. Cerlinca, T., Turcu, C., Turcu, C., & Cerlinca, M. (2010). *12 rfid-based information system for patients and medical staff identification and tracking* . Retrieved from http://cdn.intechopen.com/pdfs/8502/InTech-Rfid_based_information_system_for_patients_and_medical_staff_identification_and_tracking.pdf
25. Cavoukian, A. (2008). *Rfid and privacy*. Retrieved from http://www.hp.com/canada/portal/enterprise/downloads/rfid-healthcare.pdf
26. Li-Shiang Tsay; Williamson, A.; Seunghyun Im; , "Framework to Build an Intelligent RFID System for Use in the Healthcare Industry," *Technologies and Applications of Artificial Intelligence (TAAI), 2012 Conference on* , vol., no., pp.109-112, 16-18 Nov. 2012

    doi: 10.1109/TAAI.2012.58
27. Mosher, W. (1999). *U.S. Patent No.* 5,973,600. Washington, DC: U.S.

28. Fuhrer, P., & Guinard, D. (n.d.). Retrieved from http://www.vs.inf.ethz.ch/publ/papers/dguinard_06_smartHospital.pdf

29. Chowdhury, B., & Khosla, R. (2007). *Sixth international conference on computer and information science (icis 2007), melbourne, australia - 11-13 july 2007*. Retrieved from http://arrow.latrobe.edu.au:8080/vital/access/HandleResolver/1959.9/124367

30. Grover, A., & Berghel, H. (2011, December 12). *A survey of rfid deployment and security issues*.
Retrieved from: http://berghel.org/publications/rfid/rfid.php

31. Agarwal, A., & Mitra, M. (2006). *Rfid: Promises and problems*. Retrieved from: http://www.avoine.net/rfid/download/papers/AgarwalM-2006-pes.pdf

32. Shih, D., Lin, C., & Lin, B. (2005). Privacy and security aspects of rfid tags. Retrieved from http://swdsi.org/swdsi05/Proceedings05/paper_pdf/SWDSI-Privacy_and_Security_Aspects_of_RFID_Tags - Lin (T4D3).pdf

33. Grimaila, M. (2007). Rfid security concerns. *ISSA Journal*, Retrieved from http://www.google.com/url?sa=t&rct=j&q=rfid security issues&source=web&cd=10&cad=rja&sqi=2&ved=0CHAQFjAJ&url=http://www.slideshare.net/PeterSam67/rfid-security-concerns&ei=YXvzUNvKDIvK9QTgw4HIBA&usg=AFQjCNH4xmlSQCTf2ieejqlBJxRsgFRX4Q

34. Peris-Lopez, P., Hernandez-Castro, J., Estevez-Tapiador, J., & Ribagorda, A. (2009). ttacking rfid systems. In P. Kitsos (Ed.), *Security in RFID and Sensor Networks*Retrieved from http://0-library.ncat.edu.sheba.ncat.edu/search~S1?/X Security in RFID and Sensor Networks Security in RFID and Sensor

Networks&searchscope=1&SORT=AX&m=&b=&l=&Da=&Db=&p=/X Security in RFID and Sensor Networks Security in RFID and Sensor Networks&searchscope=1&SORT=AX&m=&b=&l=&Da=&Db=&p=&SUBKEY= Security in RFID and Sensor Networks Security in RFID and Sensor Networks/1,6,6,B/l856~b2255617&FF=X Security in RFID and Sensor Networks Security in RFID and Sensor Networks&searchscope=1&SORT=AX&m=&b=&l=&Da=&Db=&p=&5,5,,1,0

35. Bani Shemaili, M., Yoeb Yeun, C., & Jamal Zemerly, M. (2010). *Smart rfid security, privacy, and authentication*. Khalifa University for Science, Technology, and Re. Retrieved from http://cdn.intechopen.com/pdfs/8855/InTech-Smart_rfid_security_privacy_and_authentication.pdf
36. Juels, A., Rivest, R., & Szydlo, M. (2003). The blocker tag: Selective blocking of rfid tags for consumer privacy. Retrieved from http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/blocker-full/blocker-full.pdf
37. Inoue, S., & Yasuura, H. (2003). Rfid privacy using user-controllabe uniqueness. Retrieved from http://www.c.csce.kyushu-u.ac.jp/lab_db/papers/paper/pdf/2003/sozo03_5.pdf
38. Ari Juels. (2004). Minimalist cryptography for low-cost rfid tags. Retrieved from http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/minimalist/Minimalist.pdf
39. Lee, Y., & Verbauwhede, I. (2009). Secure and low-cost rfid authentication protocols. Retrieved from http://www.cosic.esat.kuleuven.be/publications/article-663.pdf

40. Storey, P., & Kolker, A. (2012). *Management engineering for effective healthcare delivery : Principles and application*. (1st ed., Vol. 1). Hershey, PA: Medical Information Science Reference.

41. Ustundag, A. (2013). *The value of rfid-benefits vs.cost*. (1st ed., Vol. 1). London, England: Springer.

42. Miles, S., Sarma, S., & Williams, J. (2008). *Rfid technology and applications*. (1st ed., Vol. 1). New York: Cambridge University Press.

43. Zhang, Y., Yang, L., & Chen, J. (2010). *Rfid and sensor networks—architectures, protocols, security, and integrations*. Boca Raton, FL: CRC Press Taylor & Francis Group.

44. Zhang, Y., & Kitos, P. (2009). *Security in rfid and sensor networks*. (1st ed.). Boca Raton, FL: CRC Press Taylor & Francis Group.

45. Karmakar, N. (2010). *Handbook of smart antennas for rfid systems*. (1st ed.). Hoboken, New Jersey: John Wiley & Sons, Inc.

46. Dobkin, D. (2013). *The rf in rfid—uhf rfid in practice, second edition*. (2nd ed.). Waltham, MA: Elsevier Inc.

47. Feder, B. (2006, April). Dealing with quirks in a metal and in the start-up game . *The New York Times*. Retrieved from http://www.nytimes.com/2006/04/27/technology/27sbiz.html?_r=0

48. Paddock, C. (2008). Retrieved from http://www.medicalnewstoday.com/articles/112877.php

49. van der Togt, R., van Lieshout, E. J., Hensbroek, R., Beinat, E., Binnekade, J. M., & Bakker, P. J. M. (2008). Retrieved from http://jama.jamanetwork.com/article.aspx?articleid=182113

50. Bauer-Reich, C., Reich, M., and Nelson, R., (2011). The Interaction of Electrostatic Discharge and RFID, Advanced Radio Frequency Identification Design and Applications, Dr Stevan Preradovic (Ed.), ISBN: 978-953-307-168-8, InTech, DOI: 10.5772/15104. Available from: http://www.intechopen.com/books/advanced-radio-frequency-identification-design-and-applications/the-interaction-of-electrostatic-discharge-and-rfid

51. Pais, S., & Symonds, J. (2011). Data storage on a rfid tag for a distributed system. *International Journal of UbiComp, 2*(2), Retrieved from http://airccse.org/journal/iju/papers/2211iju03.pdf

52. Pesonen N., Jaakkola K., Lamy J., Nummila K., and Marjonen J., (2009). Smart RFID Tags, Development and Implementation of RFID Technology, Cristina Turcu (Ed.), ISBN: 978-3-902613-54-7, InTech, DOI: 10.5772/6523. Available from: http://www.intechopen.com/books/development_and_implementation_of_rfid_technology/smart_rfid_tags

53. Poole, I. (n.d.). Retrieved from http://www.radio-electronics.com/info/wireless/radio-frequency-identification-rfid/tags-tagging-transponders-smart-labels.php

54. Fowler, D. (2013, Aug 05). Portable power: Flexible batteries. *The Engineer (Online)*, Retrieved from http://search.proquest.com/docview/1417758544?accountid=12711

55. Mandal, S.; Turicchia, L.; Sarpeshkar, R., "A Battery-Free Tag for Wireless Monitoring of Heart Sounds," *Wearable and Implantable Body Sensor Networks, 2009. BSN 2009.*

Sixth International Workshop on , vol., no., pp.201,206, 3-5 June 2009
doi: 10.1109/BSN.2009.11

56. Philipose, M.; Smith, J.R.; Jiang, B.; Mamishev, A.; Roy, S.; Sundara-Rajan, K., "Battery-free wireless identification and sensing," *Pervasive Computing, IEEE* , vol.4, no.1, pp.37,45, Jan.-March 2005
57. Perez, G.B.; Malinowski, M.; Paradiso, J.A., "An ultra-low power, optically-interrogated smart tagging and identification system," *Automatic Identification Advanced Technologies, 2005. Fourth IEEE Workshop on* , vol., no., pp.187,192, 17-18 Oct. 2005
58. D. Seetharam and R. Fletcher,; "Battery-Powered RFID", SenseID 2007 1st ACM Workshop on Convergence of RFID and Wireless Sensor. Networks and their Applications, Nov. 2007, p.1-6.
59. Dabas, C., & Gupta, J. P. (2010). A cloud computing architecture framework for scalable RFID. In *Proceedings of the International MultiConference of Engineers and Computer Scientists* (Vol. 1).
60. Zhang, T., Ouyang, Y., Li, C., & Xiong, Z. (2007, September). A scalable rfid-based system for location-aware services. In *Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on* (pp. 2117-2123). IEEE.
61. Carreton, A. L., Pinte, K., & De Meuter, W. (2010, January). Distributed object-oriented programming with RFID technology. In *Distributed Applications and Interoperable Systems* (pp. 56-69). Springer Berlin Heidelberg.
62. What is AmbientTalk about?. (2012, May 2). *[Ambient-Oriented Programming]*. Retrieved March 10, 2014, from https://soft.vub.ac.be/amop/

63. Dedecker, J., Van Cutsem, T., Mostinckx, S., D'Hondt, T., & De Meuter, W. (2006). Ambient-oriented programming in ambienttalk. In *ECOOP 2006–Object-Oriented Programming* (pp. 230-254). Springer Berlin Heidelberg.

64. Tanenbaum, A. S. (1995). *Distributed operating systems*. Pearson Education India.

65. Ni, Y., & Adviser-Kremer, U. (2006). *Programming ad-hoc networks*. Rutgers University.

66. (n.d.). Retrieved from http://health.usnews.com/best-hospitals/area

67. Dong-Sheng, L., Xue-Cheng, Z., Fan, Z., & Min, D. (2006). Embeded EEPROM memory achieving lower power-new design of EEPROM memory for RFID tag IC. *Circuits and Devices Magazine, IEEE*, *22*(6), 53-59.

68. *13.56mhz hf long distance reader dl5510* . (n.d.). Retrieved from http://www.rfid-in-china.com/2008-11-09/products_detail_2160.html

69. *Omni-directional active rfid reader*. (n.d.). Retrieved from http://www.alibaba.com/product-detail/Omni-directional-Active-RFID-Reader_559873908.html?s=p

70. Thingmagic astra-ex integrated rfid reader - poe. (n.d.). Retrieved from http://www.atlasrfidstore.com/ThingMagic_Astra_EX_Integrated_RFID_Reader_POE_p/a6-na-poe.htm

71. *Thingmagic m6 uhf rfid reader (4 port) - with ac power and wi-fi*. (n.d.). Retrieved from http://www.atlasrfidstore.com/ThingMagic_M6_UHF_RFID_Reader_4_Port_WiFi_p/m6-wifi-na.htm

72. *Alien alr-9900 enterprise rfid reader*. (n.d.). Retrieved from http://www.atlasrfidstore.com/Alien_ALR_9900_Enterprise_RFID_Reader_p/alr-9900-plus.htm

73. Auerbach, R. (2013, July 16). Top 10 hospitals in the united states. Retrieved from http://www.cnn.com/2013/07/16/health/best-hospitals-ranking/index.html

74. Singh, S. (n.d.). Indian Schools All Set To Implement RFID And GPS Based Tracking System. *InstaBlog Global Community Viewpoint and Opinion*. Retrieved June 13, 2013, from http://www.instablogs.com/indian-schools-all-set-to-implement-rfid-and-gps-based-tracking-system.html

75. . (n.d.). *Alibaba*. Retrieved March 25, 2014, from http://www.alibaba.com/trade/search?fsb=y&IndexArea=product_en&CatId=&SearchText=RFID

76. Manufacturer & Designer of RFID Smart Cards, RFID Labels, RFID Tags, RFID Readers and RFID Hotel Keycards and GPS and tracking devices. (n.d.). *Manufacturer & Designer of RFID Smart Cards, RFID Labels, RFID Tags, RFID Readers and RFID Hotel Keycards and GPS and tracking devices*. Retrieved March 25, 2014, from http://www.rfidinfotek.com

77. atlasRFIDstore is Your Source for RFID Technology. (n.d.). *Atlas RFID Store*. Retrieved March 25, 2014, from http://www.atlasrfidstore.com

78. . (n.d.). *US News*. Retrieved March 25, 2014, from http://health.usnews.com/best-hospitals/area

79. Auerbach, R. (2013, July 16). Top 10 hospitals in the United States. *CNN*. Retrieved March 25, 2014, from http://www.cnn.com/2013/07/16/health/best-hospitals-ranking/index.html